UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS

FACULDADE DE DIREITO

O CONSENTIMENTO NO ACEITE DOS TERMOS E CONDIÇÕES DE USO DOS PROVEDORES DE APLICAÇÕES DE INTERNET E A SUA RELAÇÃO COM A PROTEÇÃO DE DADOS PESSOAIS.

LETÍCIA LIMA TAVEIRA MIRANDA

Rio de Janeiro
2019 / 2° SEMESTRE

LETÍCIA LIMA TAVEIRA MIRANDA

O CONSENTIMENTO NO ACEITE DOS TERMOS E CONDIÇÕES DE USO DOS PROVEDORES DE APLICAÇÕES DE INTERNET E A SUA RELAÇÃO COM A PROTEÇÃO DE DADOS PESSOAIS.

Monografia de final de curso, elaborada no âmbito da graduação em Direito na Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do **Professor LL.M. Allan Nascimento Turano.**

Rio de Janeiro
2019 / 2° SEMESTRE

CIP - Catalogação na Publicação

Lima Taveira Miranda, Letícia
L672c O CONSENTIMENTO NO ACEITE DOS TERMOS E CONDIÇÕES DE USO DOS PROVEDORES DE APLICAÇÕES DE INTERNET E A SUA RELAÇÃO COM A PROTEÇÃO DE DADOS PESSOAIS. / Letícia Lima Taveira Miranda. -- Rio de Janeiro, 2019.
69 f.

Orientador: Allan Nacimento Turano.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade Naciona de Direito, Bacharel em Direito, 2019.

1. Consentimento. 2. Proteção de dados pessoais. 3. Termos e condições de uso. 4. Provedores de aplicação. 5. Redes sociais. I. Nacimento Turano, Allan, orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

LETÍCIA LIMA TAVEIRA MIRANDA

O CONSENTIMENTO NO ACEITE DOS TERMOS E CONDIÇÕES DE USO DOS PROVEDORES DE APLICAÇÕES DE INTERNET E A SUA RELAÇÃO COM A PROTEÇÃO DE DADOS PESSOAIS.

Monografia de final de curso, elaborada no âmbito da graduação em Direito na Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do **Professor LL.M. Allan Nascimento Turano.**

Data da Aprovação: __ / __ / ____.

Banca Examinadora:

_____
Orientador

_____
Membro da Banca

_____
Membro da Banca

Rio de Janeiro
2019 / 2° SEMESTRE

Dedico este trabalho aos meus pais, Solange e Marcelino, e às minhas irmãs, Laís, Livia e Lilian, pelo papel fundamental que exercem em minha vida. Dedido também ao meu amor, Henrique, pelo companheirismo de sempre.

RESUMO

O presente trabalho tem o intuito de analisar o disposto nos termos e condições de uso de alguns dos maiores provedores de aplicações de internet, visando compreender quais permissibilidades são fornecidas pelo usuário por meio do seu consentimento. Para que isso ocorra, será feita uma contextualização histórica, desde o surgimento da internet, passando pelas gerações de leis acerca da temática e finalizando com o debate sobre a importância da proteção de dados na nossa sociedade atual, na qual estamos emersos no apogeu das mídias sociais e da utilização dos algoritmos para diferentes funcionalidades. Além disso, também será necessário dissecar o conceito do consentimento e das suas adjetivações, com base na Lei Geral de Proteção de Dados Brasileira, bem como as implicações que a legislação trará em matéria de direitos do titular de dados. Por fim, por meio do método analítico, será analisado se esses termos de uso e políticas de privacidade estão aptos para o início dos efeitos da LGPD.

Palavras-chaves: consentimento; termos e condições de uso; redes sociais; provedores de aplicação.

ABSTRACT

The purpose of this paper is to analyze the terms and conditions of use of some of the largest internet applications providers, aiming to understand what permissibilities are provided by the user with their consent. To that end, it will be done a historical contextualization, beginning with the emergence of the Internet, passing by the laws on the subject generations, and completing with the debate on the importance of data protection in our current society, in which we are immersed in the peak of media and use of algorithms for different functionalities. In addition, it will also be necessary to dissect the concept of consent and its adjectives, based on the Brazilian General Data Protection Act, as well as the implications that the legislation will have on the data subject's rights. Finally, through the analytical method, it will be examined whether the terms of use and privacy policies fit for the introduction of LGPD effects.

Keywords: consent; terms and conditions of use; social networks; application providers.

INTRODUÇÃO.

Uma máquina de escrever, papel, caneta e livros. Parece uma realidade muito distante, todavia, há aproximadamente 25 anos, trabalhos como este estariam sendo escritos com o auxílio majoritário desses instrumentos, sem que houvesse sequer a possibilidade de realizar uma simples busca no Google.

Em um lapso temporal muito curto, os avanços tecnológicos ganharam um espaço que nem mesmo os produtores de "Os Jetsons"[1] poderiam prever. De início, veio à popularização da Internet discada e, posteriormente, da banda larga. Quem viveu os anos 2000 e a árdua missão de conectar-se à internet por meio da linha telefônica não poderia imaginar que, em menos de 10 anos, teríamos acesso a um mundo irrestrito na palma da mão.

O crescimento de tal área foi exponencial. E a sociedade, em geral, sofreu mudanças significativas, uma vez que, segundo Bruno Bioni,[2] ela "está encravada por uma nova forma de organização em que a informação é o elemento nuclear para o desenvolvimento da economia, substituindo os recursos que outrora estruturavam as sociedades agrícolas, industrial e pós-industrial".

Atualmente, principalmente após o advento da internet móvel, nosso cotidiano é permeado pela conectividade. As relações pessoais, os hábitos e as formas de interações sociais sofreram importantes impactos junto aos avanços permitidos pela tecnologia. Sem guias, manuais de instruções ou qualquer aviso prévio, a internet veio como um espaço democrático que possibilitou ao indivíduo liberdade em se comunicar e ser da forma como lhe convém.

Nesse sentido, cabe ressaltar o papel que um importante componente dessa Era Digital vem tomando como intermediador dos mais diversos tipos de interações humanas: as redes sociais.

---

[1] EM 2062, invenções do desenho Os Jetsons serão ultrapassadas. **TERRA**, 29 de outubro de 2012. Disponível em:https://www.terra.com.br/noticias/tecnologia/em-2062-invencoes-do-desenho-os-jetsons-serao-ultrapassadas,2d08a6882596b310VgnCLD200000bbcceb0aRCRD.html. Acesso em: 09 de agosto de 2019.

[2] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e o limite do consentimento. Rio de Janeiro: Forense, 2019.

Sua influência é dada nos mais diversos campos, seja na política, cultura ou no entretenimento. Acontece que, em contraponto ao domínio praticamente absoluto da sua utilização e acesso irrestrito, temos a falta de conhecimento e preocupação quanto ao gerenciamento do rastro virtual deixado por cada usuário ao utilizar-se de um provedor na Internet.

O usuário médio, quando acessa redes sociais como Facebook, Twitter e Intagram, não possui o dimensionamento do quanto está fornecendo de informações e do viés para o qual elas estão sendo utilizadas. A partir da sua coleta, passando pela mineração e processamento, é possível chegarmos numa formação de amostras, utilizada atualmente por diversos setores da economia mundial, visando personificar e entender com profundidade o perfil do propenso consumidor.

Banaliza-se socialmente a importância da vida privada do indivíduo comum em comparação a outros cidadãos, sob os quais a vida notória teria mais relevância. Mas, é fato que todos temos aspectos sob os quais gostaríamos de manter sigilo, e é dentro dessa prespectiva o presente trabalho visa se debruçar.

A pesquisa tem como objetivo geral analisar o consentimento tácito do usuário no aceite dos termos e condições de uso de plataformas na Internet, bem como inseri-lo no contexto de regulação da Lei Geral de Proteção de Dados.

Isso porque, tais termos e condições de uso são feitos no formato de um contrato de adesão, no qual o provedor condiciona a utilização da rede pelo usuário à sua concordância com os inúmeros apontamentos ali feitos, dada por meio de um mero clique.

Dessa forma, questiona-se até que medida o usuário tem acesso ao que foi fornecido como dado ao provedor. O usuário tem alguma gerência sobre o conteúdo e a duração dessa informação coletada? Esses dados podem ser disponibilizados para terceiros sem avisos prévios aos usuários? Como essa utilização de dados é exposta pelo provedor de internet? São algumas das problemáticas que pretendem ser analisadas.

Nesse sentido, dentre os objetivos específicos, estão: a verificação da forma como os termos e condições de uso explicitam a exploração e o tratamento dos dados pessoais ao

usuário; a identificação de mecanismos de controle dos dados ao usuário e como ocorre sua aplicabilidade na plataforma; análise dos tipos de dados pessoais tratados e como ocorre essa diferenciação no tratamento; verificação do prazo de duração para o tratamento e armazenamento dos dados pessoais pelos provedores; observar a presença de termos abertos ou genéricos na redação dos termos e condições de uso.

Em tempos de exposição midiática desenfreada, a privacidade torna-se cada vez mais escassa. Entretanto, de fato, tal direito à personalidade é resguardado pelo próprio texto constitucional, o que implica o dever de proteção do nosso ordenamento jurídico.

Nesse sentido, a justificativa temática do presente projeto tangencia esse universo de vigilância sobre o qual estamos emersos e até que ponto temos controle sobre ele. Principalmente, após o escândalo do caso da empresa de consultoria, *Cambridge Analytica*, que se utilizou de dados pessoais indevidamente obtidos de usuários do Facebook para promover o candidato Donald Trump na eleição norte-americana para a presidência.

Assim, busca-se, em consonância com a Lei Geral de Proteção de Dados, promulgada em Agosto de 2018, analisar a exploração dos dados pelos provedores de aplicação na Internet[3], visando compreender a permissibilidade fornecida pelo usuário e a sua utilização.

Como forma de metodologia, será utilizada a análise documental e empírica, uma vez que os resultados obtidos serão baseados nas redações dos termos e condições de uso dos provedores de aplicação na Internet. O método indutivo, por sua vez, estará presente por tratar-se de pesquisa acadêmica na qual o conhecimento de certo número de dados singulares fará com que se estabeleça uma verdade universal. Como método de procedimental, fez-se uso do método histórico no início do trabalho, especialmente ao relatar a historicidade da Internet, além do método comparativo, ao analisarmos os termos e condições de uso de diferentes plataformas.

Os provedores que serão objetos de pesquisa do trabalho em comento são: Facebook,

[3] Conforme disposto no art. 5º, VII do Marco Civil da Internet, aplicações de internet são "o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet". Em outras palavras, são os sites, as redes sociais, aplicativos e outras funcionalidade que muitas vezes coletam dados pessoais dos usuários ou para os quais o próprio usuário transmite seus dados.

Instagram, Linkedin e o Twitter. Tal escolha baseia-se no fato de que essas são algumas das redes sociais mais utilizadas no país, de forma que a sua análise possui pertinência social.

Além disso, tratam-de provedores de aplicação, ou seja, aqueles que disponibilizam funcionalidades ao usuário e possuem controle sobre o que é publicado por esse. Redes sociais com criptografia de ponta a ponta, por exemplo, dificultariam a compreensão do fornecimento dos dados pessoais.

Com base nisso, o presente trabalho divide-se em três capítulos. Para iniciar o estudo proposto, é necessário compreendermos, criticamente, como a evolução da internet influenciou a vida do indivíduo, principalmente, após o surgimento da redes sociais. Além disso, verificaremos a maneira pela qual elas estão proporcionando sua participação efetiva na sociedade e as consequências disso.

No primeiro capítulo, iremos, portanto, discorrer acerca desse ponto, analisando, de forma contextualizada, o papel exercido pelo Direito nesse processo a partir da evolução histórica das legislações sobre a temática no mundo, desde a primeira geração de leis, passando pela experiência latino-americana, até chegarmos na legislação mais completa e moderna do planeta: a GDPR.

Essa legislação, por sua vez, influenciou a chegada de uma normativa que versasse especificamente sobre a proteção de dados no Brasil. Assim, entenderemos como surgiu a Lei 13.704 de 2018, conhecida como LGPD e quais outros fatores ocorridos no período propiciaram o seu advento.

Discorrido esse ponto, aprofundaremos nossa análise no segundo capítulo. Entendida a dicotomia entre a utilização massificada dos recursos tecnológicos e a exposição que ela implica aos indivíduos na rede, bem como o porquê da proteção de dados pessoais estar tão em voga ultimamente, abordaremos os mecanismos de concretude ao princípio da autodeterminação informacional, bem como analisaremos os requisitos, elementos e formas de obtenção de uma de suas balizas: o consentimento do usuário.

Assim, passaremos para a análise do outro lado da moeda, com um exame detalhado dos termos e condições de uso das redes sociais mais relevantes no país. O objetivo desse

estudo é compreender como são estabelecidos os parâmetros para o tratamento de dados, buscando examinar as previsões expostas e o que isso implica ao usuário, correlacionando com o disposto na Lei Geral de Proteção de Dados.

1. O IMPACTO DAS REDES SOCIAIS NA SOCIEDADE DA INFORMAÇÃO.

Antes do seu nascimento, a internet (*Web 1.0*) era um espaço restrito apenas a leitura do conteúdo, o que permitia, pela primeira vez, um acesso facilitado a uma grande quantidade de informação.

O surgimento das redes sociais e dos blogs fomentou o processo de transição para a *Web 2.0*, conhecida como *"Web of communication",* na qual os usuários tiveram a oportunidade de alimentar as plataformas com informações, além de permitir a interação entre os seus membros, deixando de serem meros consumidores de conteúdo, como ocorria na *Web 1.0 –"Web of knowledge"–*, para efetivamente se tornarem produtores.

A possibilidade de comunicação e criação de conteúdo, juntamente com outros fatores, como a própria expansão do uso da internet sem fio, criou o terreno perfeito para a popularização e domínio das redes sociais no mundo.

Quanto aos seus efeitos comportamentais, a percepção é notória na sociedade. Seja no transporte público, nos restaurantes ou áreas de lazer, o celular virou um acessório primordial para grande parte da população. E o compartilhamento de dados, por consequência, cada vez maior.

Acontece que, em contraponto ao domínio praticamente absoluto da sua utilização e do seu acesso irrestrito, temos a falta de conhecimento e preocupação quanto à veracidade do conteúdo acessado e, principalmente, quanto ao gerenciamento do rastro virtual deixado por cada usuário ao utilizar-se de um provedor na Internet.

E as redes sociais, nesse sentido, possuem protagonismo nas diversas mudanças ocorridas no mundo desde então, seja no campo político, ideológico ou social.

Basta analisarmos que os mais recentes processos eleitorais pelo mundo têm sofrido influência direta da atuação dos eleitores nessas redes. Grupos de apoio a candidatos, páginas de adeptos às plataformas políticas e equipes de marketing e propaganda se utilizam desse meio para alcançar um número maior de eleitores simplesmente pelas curtidas, compartilhamentos e preferências manifestadas em suas navegações.

O risco que se apresenta, contudo, é o da deturpação desse mecanismo de acesso e divulgação de informações. Desde 2016, quando da realização das eleições presidenciais nos Estados Unidos da América, o fenômeno das "*fake news"* é pauta jornalística, eleitoral e popular, dada a capacidade de informações falsas captarem usuários que as compartilhem deliberadamente, despidos de um critério básico de verificação da procedência da informação.

O mesmo fator pode ser observado em 2018, nas eleições brasileiras[4], em que grupos vinculados a determinados candidatos usavam de notícias inverídicas para depreciar seus opositores imediatos, bem como inserir falsas informações acerca dos seus planos de governo.

Noutro giro, movimentos políticos urbanos insurgentes[5] também tem sua parcela de mobilização por meio de redes sociais. Observou-se durante as jornadas de junho, em 2013, por todo o Brasil, a capacidade da juventude se organizar em passeatas, ocupações e manifestos mediante simples eventos de Facebook, vídeos de divulgação no YouTube e fotos acessíveis a milhões de usuários no Twitter.

Em outros países, essa forma de divulgação foi aplicada com o mesmo intuito, vide "*Occupy Wall Street*", nos EUA, a Primavera Árabe contra as ditaduras em países como Egito, Líbia, Tunísia, e os mais recentes protestos contra e a favor do "*Brexit"*, a saída do Reino Unido da União Europeia.

Embora não seja comum a todas as gerações, mesmo porque se trata de um meio desenvolvido sofisticadamente há pouco tempo, o uso da internet engloba cada vez mais pessoas de outras faixas etárias que não cresceram utilizando os aparelhos e tecnologias atuais, mas que se adequaram à realidade que as permeia. Desse modo, não há, inclusive, como ignorar um avanço que praticamente extirpou outros métodos de comunicação, devido à sua rapidez, facilidade de acesso e preço.

---

[4] GRAGNANI, Juliana. Um Brasil dividido e movido a notícias falsas: uma semana dentro de 272 grupos políticos no WhatsApp. **BBC News Brasil**, Londres, 05 de outubro de 2018. Disponível em: https://www.bbc.com/portuguese/brasil-45666742. Acesso em: 09 de agosto de 2019.

[5] HOLSTON, James. Rebeliões metropolitanas e planejamento insurgente no século XXI | Insurgent cities and urban citizenship in the 21st Century. **Revista Brasileira de Estudos Urbanos e Regionais**, [S.l.], v. 18, n. 2, p. 191, ago. 2016. ISSN 2317-1529. Disponível em: http://rbeur.anpur.org.br/rbeur/article/view/5162. Acesso em: 09 agosto de 2019.

Mais uma interface das redes sociais na sociedade de informação se relaciona com o rompimento de formalidades no âmbito da comunicação social. Por exemplo, anos atrás a televisão era o único meio utilizado para pronunciamentos oficiais, entrevistas e divulgação de informações de interesse público e/ou relacionados às novas tendências de empresas, táticas de mercado, etc.

Hoje em dia, opera-se a substituição desse formato, com a televisão detendo um uso cada vez mais complementar, subsidiário, e as redes sociais, bem como os sites oficiais de marcas e instituições, servindo como plataforma de veiculação das suas práticas e lançamentos.

O efeito positivo dessa dinâmica é a capacidade de comunicação direta entre usuários e fornecedores, cidadãos e órgãos públicos, eleitores e políticos, notadamente pela possibilidade do exercício de uma espécie de pressão social que lhes retira da passividade antes assumida na qualidade de telespectador, para a efetiva contribuição e participação naquilo que lhes interessa.

Nesse sentido, demandas populares, manifestos políticos e rejeições a determinadas medidas ganham robustez pelas redes sociais. Como exemplo recente, a própria anulação da nomeação de Ilena Szabó[6] para chefiar o Conselho de Política Criminal e Penitenciária, horas após sua indicação pelo Ministro da Justiça e Segurança Pública, Sérgio Moro, por possuir ideias não partilhadas por eleitores do atual presidente do Brasil, Jair Bolsonaro.

Ressalta-se que não são apenas os usuários que utilizam as tecnologias para aperfeiçoar os seus modos de agir e pensar atualmente. Além da *Web 2.0*, mencionada anteriormente, já é desenvolvida e aplicada na rede mundial de computadores a chamada *Web 3.0.*[7].

Nesse formato, as preferências, os comportamentos rotineiros e as buscas frequentes dos usuários são processados a partir de algoritmos, os quais projetam o que interessa às pessoas

[6] VENAGLIA, Guilherme. Após crítica de bolsonaristas, Moro volta atrás em nomeação de Ilona Szabó. **VEJA**, 28 de fevereiro de 2019. Disponível em: https://veja.abril.com.br/politica/apos-critica-de-bolsonaristas-moro-volta-atras-em-nomeacao-de-ilona-szabo/. Acesso em: 09 de agosto de 2019.
[7] Markoff, John. **Entrepreneurs see a web guided by common sense.** The New York Times, 2006. Disponível em: https://www.nytimes.com/2006/11/12/business/12web.html. Acesso em: 09 de agosto de 2019.

em qualquer página que abram, seja para pesquisa, rede social, aplicativo, etc.

Essa nova "geração" da internet, dita terceira onda, impacta diversos setores, desde negócios, mercado consumidor, até a exclusão ou omissão daquilo que, em tese, se contrapõe ao que é relevante para quem está utilizando o meio informatizado. A ressalva a ser feita quanto ao uso do algoritmo é a capacidade do usuário em determinar o que está sendo usado de informação própria e para qual fim.

1.1 Porque proteger os dados pessoais?

Por que estamos dando tamanha importância aos dados pessoais? Essa é uma pergunta feita por grande parte da população quando se depara com um noticiário abordando questões sobre o assunto.

Talvez, tal dúvida tenha suas razões para existir: seja pela ausência de um debate em nível mais popular; seja pela maior parte da produção acadêmica ser feita em outro idioma que não o português; seja pela complexidade na cognição dos termos utilizados ou, até mesmo, pela irrelevância ainda dada pela sociedade, que menospreza o interesse econômico dado às próprias informações quando comparado, por exemplo, à relevância da privacidade de figuras públicas[8].

Mesmo subjugando os seus dados, por trás da assertiva do "eu não tenho nada a esconder", uma coisa é certa: todos se incomodariam se, no momento de abrirem a caixa de correspondência de suas respectivas casas, descobrissem que cartas pessoais, contas e afins foram violadas.

Mas, por qual motivo o direito à privacidade na Internet ainda é algo tão mitigado pela população brasileira? Por que a indignação é mais seletiva nesses casos, se a rede social pode

[8] Nesse sentido, "a proteção à intimidade não pode ser exaltada a ponto de conferir imunidade contra toda e qualquer veiculação de imagem de uma pessoa, constituindo uma redoma protetora só superada pelo expresso consentimento, mas encontra limites de acordo com as circunstâncias e peculiaridades em que ocorrida a captação". BRASIL. Recurso Especial nº 595.600 - SC. Superior Tribunal de Justiça. Direito civil. Direito de imagem. *Topless* praticado em cenário público. Recorrente: Maria Aparecida de Almeida Padilha. Recorrido: Zero Hora Editora Jornalística S/A. Relator: César Asfor Rocha. Brasília, 18 de março de 2004. Disponível em: https://ww2.stj.jus.br/websecstj/cgi/revista/REJ.cgi/ATC?seq=1160972&tipo=5&nreg=200301770332&SeqCgrmaSessao=&CodOrgaoJgdr=&dt=20040913&formato=PDF&salvar=false. Acesso em: 20 de agosto de 2019.

propiciar mais informações sobre você do que a própria caixa de correios?

Conforme exposto na introdução de sua obra, Danilo Doneda[9] afirma que:

> "A tutela da privacidade como 'direito a ser deixado só', associada ao isolamento, à reclusão, não nos permite determinar parâmetros para julgar o que ela representa em um mundo no qual o fluxo de informações aumenta incessantemente, assim como aumenta o número de oportunidades de realizarmos escolhas que podem influir na definição da nossa esfera privada. As demandas que moldam o perfil da privacidade hoje são de outra ordem, relacionadas à informação e condicionadas pela tecnologia".

Na mesma toada, Stefano Rodotà[10] expõe que:

> "Se este é o quadro global a ser observado, não é mais possível considerar os problemas da privacidade somente por meio de um pêndulo entre 'recolhimento' e 'divulgação'; entre o homem prisioneiro de seus segredos e o homem que nada tem a esconder; entre a 'casa-fortaleza', que glorifica a privacidade e favorece o egocentrismo e a 'casa-vitrine', que privilegia as trocas sociais; e assim por diante. Essas tendem a ser alternativas cada vez mais abstratas, visto que nelas se reflete uma forma de encarar a privacidade que negligencia justamente a necessidade de dilatar esse conceito para além de sua dimensão estritamente individualista, no âmbito da qual sempre esteve confinada pelas circunstâncias de sua origem."

Neste sentido, a esfera de defesa da privacidade não mais se resume ao seu aspecto individualista e negativo, no qual a mera abstenção do Estado ou de terceiros é o suficiente para que não ocorra a sua violação. A realidade fática exige uma maior proteção, tendo em vista a suscetibilidade das nossas informações na Era Digital.

Sem teorias conspiratórias ou futurísticas, e sim, baseada nas demandas do século em que vivemos, podemos afirmar que os dados são, hoje, o interesse mercadológico predominante, tanto do setor público quanto do setor privado. Isso porque, como já dizia Yuval Noah Harari[11], por meio de algoritmos eletrônicos, é possível "refiná-los em informação, informação em conhecimento e conhecimento em sabedoria".

---

[9] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.
[10] RODOTÀ, Stefano. **A vida na sociedade de vigilância - a privacidade hoje.** Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro. Renovar, 2008.
[11] HARARI, Yuval Noah. **Homo Deus:** uma breve história do amanhã. Tradução: Paulo Geiger. 1ª edição. São Paulo: Companhia das Letras, 2006.

E essa sabedoria, por sua vez, assume importância por dois pressupostos diversos: "o controle e a eficiência" [12]. Por meio da coleta e tratamento, nossos dados são usados para atender a interesses comerciais e estatais com um grau de precisão nunca antes alcançado. E que, por vezes, ultrapassam limites éticos e legalmente aceitos.

Isso porque, por meio das informações geradas a partir da análise dos nossos dados, perfis comportamentais são traçados com grande precisão acerca das nossas escolhas, cada vez mais individualizados e perfeitos para o exercício de um controle mais específico e eficiente.

Nesse sentido, a regulamentação sobre a proteção de dados pessoais é necessária para entendermos como se deu a construção dessa baliza entre a privacidade do usuário e o avanço informático, e se, de fato, estamos protegendo sem necessariamente engessarmos o progressoem tal área.

No próximo tópico, adentraremos no surgimento das legislações mais importantes e influentes sobre o tema, com enfoque nas suas discussões ao longo do tempo.

1.2. A evolução da legislação sobre dados pessoais no mundo.

O avanço tecnológico nos parece, à primeira vista, algo recente no contexto histórico, principalmente pelos exorbitantes avanços que tivemos nos últimos dez anos, os quais são tão fundamentais no nosso cotidiano, que questionamos como vivíamos antes de tantas ferramentas facilitadoras.

Nesse sentido, diferente do que poderíamos imaginar, a legislação pioneira sobre dados pessoais surgiu há cerca de 50 anos. Trata-se da Lei de Proteção de Dados do Estado Alemão de Hesse – *hessisches Datenschutzgesetz* [13] –, criada no contexto do pós-guerra, com a superação dos regimes autoritários, a fundação de um Estado Moderno, a expansão industrial, bem como o avanço computacional nos países desenvolvidos.

Por mais que a legislação tivesse sido estabelecida em 1970, sua entrada em vigor só se

[12] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.
[13] ALEMANHA. *Hessisches Datenschutzgesetz*, de 7 janeiro de 1999.

deu ao final do século, em 1979. E durante esse lapso temporal, outros diplomas surgiram, como o Ato de Dados Sueco – *Sw. Datalagen*[14]–, primeira lei em âmbito nacional.

De acordo com Renato Leite Monteiro[15], a lei sueca e a lei de Hesse guardam similaridades, como, por exemplo, uma formulação mais genérica, sem previsões quanto às situações nas quais a coleta de dados poderia ou não ocorrer, nem quanto aos princípios gerais do tratamento de dados pessoais, tratados de maneira muito ampla e abstrata nesse primeiro momento. No entanto, conforme exposto pelo autor, a "lei inovou ao trazer o tema da proteção de dados dos cidadãos para a agenda pública de governo".

No mesmo período, outras importantes legislações foram surgindo pelo território europeu, como na Dinamarca e na Alemanha em âmbito federal, ainda no formato pouco abrangível das pioneiras. Além das mencionadas, temos o *Privacy Act* norte-americano.

Tais leis são conhecidas como "de primeira geração", numa classificação utilizada pela doutrina. A intenção primordial na criação de um regulamento específico era travar o avanço estatal no controle das informações pessoais de seus cidadãos, que percebendo a efetividade que poderia ser alcançada com a formação de bancos de dados unificados, criou propostas nesse sentido.

Segundo Danilo Doneda[16], esse momento seria "focalizado basicamente na atividade de processamento de dados", marcado pela presença de "regras concretas e específicas dirigidas aos agentes diretamente responsáveis" e "sem prever a participação do cidadão nesse processo". Nessa perpectiva, Bruno Bioni[17] complementa ao afirmar que essa primeira geração foi marcada pela "premissa em se estabelecer normas rígidas que domassem o uso da tecnologia".

Logo essas leis tornaram-se ultrapassadas, devido à burocracia que não acompanhava as

---

[14] SUÉCIA. *Sw. Datalagen*, de 11 de maio de 1973.
[15] MONTEIRO, Renato Leite. **Lei Geral de Proteção de Dados e GDPR: histórico, análise e impactos.** Disponível em: https://baptistaluz.com.br/wp-content/uploads/2019/01/RD-DataProtection-ProvF.pdf. Acesso em: 06 de agosto de 2019.
[16] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.
[17] BIONI, Bruno Ricardo. **Proteção de dados pessoais:** a função e o limite do consentimento. Rio de Janeiro: Forense, 2019.

inúmeras inovações nas formas de processamento de dados e a fragmentação no tratamento feito por terceiros, o que exigia uma nova estrutura normativa.

Surgiram, então, as leis de "segunda geração", baseadas na "consideração da privacidade e na proteção dos dados pessoais como uma liberdade negativa, a ser exercitada pelo próprio cidadão" [18]. Uma de suas características, além da mudança na figura do processador de dados, que transcendeu do agente estatal para o setor privado, é a necessidade de se obter o consentimento do cidadão para utilizar-se dos seus dados.

Como exemplos, podemos citar a lei austríaca [19] e a lei francesa [20], além das constituições portuguesa[21] e espanhola[22], que reconheciam, já naquela época, a privacidade como um direito fundamental.

Ocorre que, atribuir à proteção de dados o caráter meramente negativo não trouxe benefícios para o usuário, uma vez que apenas restringiu o seu papel, cabendo a ele a aceitação ou não da utilização dos seus dados. Dessa maneira, caso houvesse a recusa no processamento de suas informações, o único lesado era o indivíduo que deixava de utilizar a plataforma.

No mais, as ferramentas propiciadas pela tecnologia tornaram-se essenciais no cotidiano. E, nessa toada, transferir para o usuário a responsabilidade pela não conformidade do tratamento de seus dados pelo provedor significa excluí-lo digitalmente e, consequentemente, do ambiente social.

Assim, com a "mudança do paradigma tecnológico" [23], sobrevieram as leis de "terceira geração", numa tentativa de melhor proteger o cidadão no ambiente virtual, sem que ele precisasse abrir mão do seu uso, passando, portanto, a "abranger mais do que a liberdade de fornecer ou não seus dados pessoais, preocupando-se também em garantir a efetividade desta

[18] DONEDA, op. cit, p. 219.
[19] *Datenschutzgesetz*, de 18 de outubro de 1978.
[20] *Loi Informatique, Fichiers et Libertés*, de 6 de janeiro de 1978.
[21] Constituição da República Portuguesa, de 25 de abril de 1976.
[22] Constitución española, de 29 de agosto de 1978.
[23] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.

liberdade” [24].

A partir de tal geração, surgem alguns mecanismos de autotutela, propiciando aos usuários meios próprios para zelar pela sua liberdade informacional, além de garantir o efetivo exercício da autodeteterminação informacional. Bruno Bioni[25], ao discorrer sobre o assunto, afirmou que, nesse estágio, “as normas de proteção aos dados pessoais procuraram assegurar a participação do indivíduo sobre todos os movimentos dos seus dados pessoais: da coleta ao compartilhamento”.

De acordo com Danilo Doneda, essa linhagem diferencia-se das outras gerações pela "participação ativa e consciente nas fases sucessivas do processo de tratamento e utilização de sua própria informação por terceiros.” Importante ressaltar que o cenário se deu na década de 1980.

Ocorre que, questionar e colocar em prática a autonomia informacial, demanda um custo que não pode ser suprido por todos os indivíduos que se utilizam da Internet, o que acabava por limitar o seu espaço de ação e, portanto, a efetividade esperada.

Diante desse quadro de hipossuficiência entre o usuário e o provedor, se fez necessária a criação de meios que propiciassem um equilíbrio entre as duas partes. Entendeu-se importante para suprir tal deficiência da norma, a criação de instrumentos que privilegiassem a tutela coletiva frente às “desvantagens do enfoque individual existente até então”[26].

Nesse sentido, na “quarta geração”, buscou-se uma “forte dose de pragmatismo, voltado para a busca de resultados concretos”, com a disseminação das autoridades independentes responsáveis por resguardar a devida aplicação da legislação; a criação de normativa específica para o tratamento de dados de alguns setores que demandam particularidades, como o da saúde e o do crédito; e a vedação feita por algumas legislações quanto ao tratamento de dados sensíveis.

[24] Ibid.
[25] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e o limite do consentimento. Rio de Janeiro: Forense, 2019.
[26] DONEDA, op. cit., p. 304.

Mesmo com toda evolução geracional ocorrida em consonância com os avanços da informática, o papel do consentimento como vetor para o tratamento de dados não foi coadjuvante nesse quadro, sendo reafirmado e reinventado no decorrer das décadas até os dias atuais, no qual ganhou adjetivações e requisitos.

Numa tentativa de unir as diretrizes principais para uma legislação que verse sobre dados pessoais, pensando, principalmente, na perspectiva do mundo globalizado e no fluxo de informações comerciais, foram criadas iniciativas regulatórias internacionais, como os documentos emitidos pela OCDE – *Privacy guidalines*, em 1980, e *declaration on transborder data flows*, em 1985.

De acordo com o Prefácio das *guidalines*, uma das preocupações da Organização era justamente o perigo de que disparidades nas legislações nacionais pudessem dificultar o livre fluxo de dados pessoais através das fronteiras; esses fluxos aumentaram bastante nos últimos anos e devem crescer ainda mais com a introdução generalizada de novas tecnologias de computadores e comunicações, e restrições nesse sentido poderiam causar sérias perturbações em setores importantes da economia, como bancos e seguros.

Assim, tais normativas continham definições importantes sobre o tema – como a conceituação do dado pessoal e da figura do controlador de dados[27]. Também estabeleceu princípios basilares e mecanismos concretos para garantia da autodeterminação informacional, como a possibilidade cedida ao titular de apagar e retificar seus dados armazenados pelo provedor.

Mesmo com as alterações ocorridas no seu texto, em 2013, as ideias principais permaneceram intactas, apenas com alterações pontuais por conta dos avanços tecnológicos ocorridos no decorrer dos 30 anos dos quais a norma não sofreu alterações.

Isso demonstra a influência "da elevação do titular de dados pessoais como principal ator da dinâmica normativa sobre proteção de dados pessoais" e o "papel de destaque que o

[27] "1. *For the purposes of these Guidelines: 'data controller' means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf; b) 'personal data' means any information relating to an identified or identifiable individual (data subject)."* ***OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data****, on 23 September 1980.*

consentimento dos dados desempenha nesse arranjo normativo".

1.2.1. A progressão normativa dos dados pessoais na América Latina.

No cenário latino-americano, a realidade é bem diferente do que o encontrado no âmbito europeu e norte-americano. Dentre os doze países pertencentes ao continente, nem todos possuem regulamentação geral sobre a proteção dos dados pessoais, a exemplo da Guiana, do Suriname, da Bolívia e do Equador. Em geral, as leis são setoriais, como, por exemplo, no Paraguai, que conta com a *Ley nº 1.682* que *Reglamenta la Información de Carácter Privado*[28].

O primeiro país a entrar em consonância com a realidade vivida pelos países europeus foi o Chile, em agosto de 1999, ao promulgar a Ley de Protección de Datos de Carácter Personal[29]. Com os anos, a lei vem necessitando de adaptação conforme os parâmetros estabelecidos pela GDPR e OCDE.

Em seguida, veio a Argentina, com a *Ley de Protección de los Dados Personales*[30], de outubro de 2000. Atualmente, o seu nível adequado de proteção é reconhecido, juntamente ao Uruguai, com a certificação de segurança no tratamento de dados pessoais pela União Europeia, o que é importante sob a perspectiva de facilitar a transferência internacional de dados e em adequar-se aos padrões internacionais.

No mesmo período, Peru[31], Colômbia[32] e Uruguai[33] vigoraram suas legislações, trazendo disposições acerca dos princípios do tratamento dos dados pessoais e dos direitos e deveres dos titulares.

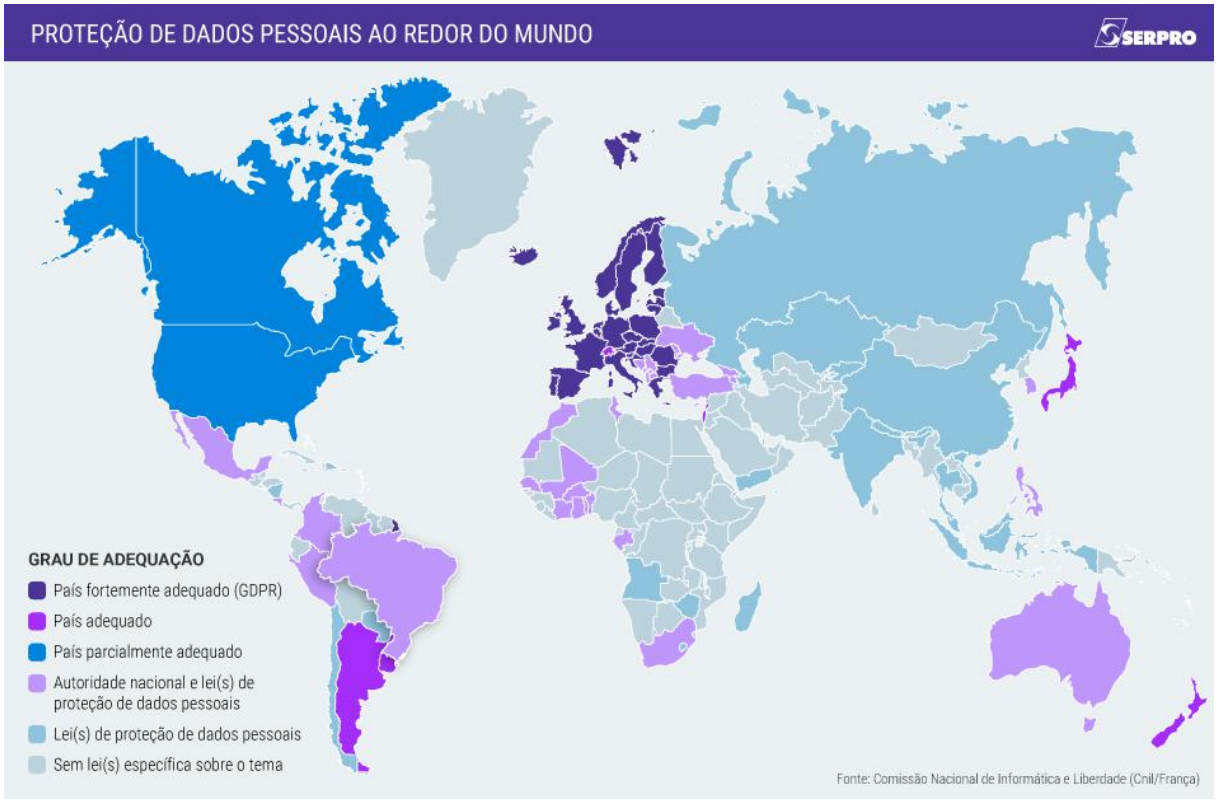
Nessa toada, mesmo com a discussão do anteprojeto de lei, em 2010, apenas recentemente, em 2018, com a sanção da Lei nº 13.709, de 14 de agosto de 2018, o Brasil entrou no rol de países com legislação própria sobre a temática, como podemos observar por

---

[28] PARAGUAI, Ley Nº 1682, de 16 de janeiro de 2001
[29] CHILE, Ley Nº 19.628, de 28 de agosto de 1999.
[30] ARGENTINA, Ley Nº 25.326, de 4 de outubro de 2000.
[31] PERU, Ley Nº 29.733, de 03 de julho de 2011.
[32] COLÔMBIA, Ley Estatutaria Nº 1.581, de 17 de outubro de 2012.
[33] URUGUAI, Ley Nº 18.331, de 18 de agosto de 2008

meio da Figura 1, que versa sobre o panorama mundial dos países que possuem legislações próprias sobre proteção de dados e o seu grau de adequação.

Figura 1 - Mapa da Proteção de Dados Pessoais ao redor do mundo.



Fonte: Comissão Nacional de Informática e Liberdade (Cnil/França)

Tal quadro demonstra a chegada tardia do país na regulamentação, que até o momento só havia previsão em leis esparsas, a exemplo de breves disposições no Código Civil, Código de Defesa do Consumidor, Lei do Cadastro Positivo, Marco Civil da Internet, dentre poucos outros textos legais.

E, nesse sentido, somos novamente um dos últimos países a incorporar o sistema legal de proteção de dados no bloco continental, o que demonstra a necessidade do direito em caminhar junto à tecnologia e oferecer soluções em tempos muito mais satisfatórios.

1.2.2. Da Convenção 108 ao General Data Protection Regulation.

Em 1981, foi promulgada pelo Conselho da Europa, a Convenção de Strasbourg, “para

proteção de indivíduos relativamente ao tratamento de dados de caráter pessoal" [34], na qual todos os países signatários deveriam editar leis nacionais em conformidade com seus princípios.

De acordo com seu preâmbulo, a finalidade desejável era:

> "alargar a proteção dos direitos e das liberdades fundamentais de todas as pessoas, nomeadamente o direito ao respeito pela vida privada, tendo em consideração o fluxo crescente, através das fronteiras, de dados de carácter pessoal susceptíveis de tratamento automatizado."

Dentre as suas previsões, está a garantia aos indivíduos, independente da sua nacionalidade ou residência, do respeito pelos seus direitos e liberdades fundamentais, em especial, pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito[35].

Apesar da influência exercida pelas diretrizes da Convenção, estas, por sua vez, não possuíam força coercitiva e nem trouxeram definições importantes sobre o tratamento de dados, o que permitiu a continuidade de uma variação considerável entre o direito interno de cada país. Além desse fator, algumas leis nacionais já haviam sido implementadas anteriormente, o que dificultava o cumprimento do seu objetivo inicial.

Com a formação do bloco da União Europeia, a partir do Tratado de *Maastricht*, foi editada a Diretiva 46/95/CE[36], um marco no campo da proteção de dados. A partir dela, foi estabelecida "uma disciplina única sobre transferência de dados a ser obedecida pelos países-membros da União Europeia e transposta para os respectivos ordenamentos nacionais"[37].

A norma dispunha de definições importantes para a temática[38], necessárias para oferecer uma maior segurança jurídica, tal como a conceituação dos dados pessoais e do seu

---

[34] França, 1981.Disponível em: https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm. Acesso em: 12 de setembro de 2019.
[35] Artigo 1º, Convenção de Strasbourg, de 1981.
[36] Luxemburgo, 24 de Outubro de 1995. Directiva 95/46/CE do Parlamento Europeu e do Conselho, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046. Acesso em: 12 de agosto de 2019.
[37] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.
[38] Artigo 2º, Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995.

tratamento; da figura do controlador; do subcontratante; do o terceiro; e do consentimento, entendido como qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa aceita que dados pessoais que lhe digam respeito sejam objeto de tratamento.

Com relação ao consentimento, a Diretiva trouxe adjetivações que conferiram concretude à autonomia informacional na tentativa de operacionalizá-lo. Nas palavras de Bruno Bioni[39]:

> "[…] a diretiva irá impor não só o direito do titular dos dados pessoais controlá-los, mas, simetricamente, deveres aos data controlares - quem processa os dados pessoais - para aperfeiçoar tal estratégia regulatória."

Quanto aos efeitos internacionais da norma, é importante salientar que, de acordo com o exposto no seu texto, era vedada a transferência de dados para países fora do bloco econômico que não possuíssem um nível "adequado" de proteção. Tal restrição tinha como objetivo fomentar a adaptação de países terceiros, "como uma forma indireta de obter eficácia extraterritorial para a própria lei europeia"[40].

A Diretiva vigorou até maio de 2018, quando sobreveio o Regulamento Geral de Proteção de Dados da União Europeia - *General Data Protection Regulation* -, em 27 de abril de 2016[41], um novo paradigma de proteção de dados não mais restrito ao território europeu. Sua abrangência e padrão legislativo são considerados os mais modernos e compatíveis com as novas tecnologias de inteligência artificial, internet das coisas e computação.

Dada a relevância do mercado europeu, a normativa europeia afeta outros cenários importantes, como o Brasil. Nesse sentido, a necessidade de um legislação que alcance os parâmetros estabelecidos é primordial para um contexto de investimento e crescimento no setor.

1.3. Contexto histórico da aprovação da LGPD e suas inovações.

A Lei Geral de Proteção de dados foi promulgada em julho de 2018 e passará a produzir

---

[39] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e o limite do consentimento. Rio de Janeiro: Forense, 2019.
[40] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar, 2006.
[41] Bruxelas, 27 de abril de 2016. Regulamento nº 2016/679.

efeitos contados 18 meses da sua sanção. Contudo, a análise de seus impactos e a influência em outras searas – econômica, política e social – não se restringem aos dispositivos legais, razão pela qual este tópico abordará o contexto em que se inseriu a proteção de dados no Brasil, quais as matrizes que serviram de inspiração para a nossa legislação, bem como os avanços promovidos por essa regulamentação.

Não se pode duvidar de um aspecto essencial da Lei 13.709/18, qual seja, sua contemporaneidade. Com a queda da União Soviética, em 1990, e a ascensão do neoliberalismo, promovido, especialmente, pelo Consenso de Washington, como uma forma de tornar o capitalismo efetivamente hegemônico no mundo, a globalização se tornou o dorso da economia mundial, pautando a atuação das nações em âmbito nacional e internacional.

Desse modo, surgiu a necessidade de aprimoramento dos meios tecnológicos, visando a otimização das formas de comunicação e acesso a serviços, em um claro exemplo do que se denominou racionalidade administrativa. Com o advento dos anos 2000, commodities, ainda que essenciais, não eram mais o objeto de desejo no comércio exterior. Gradativamente, a dinâmica do mercado buscou novas formas de produzir e fornecer serviços, aliada aos modelos de relação social que eram tecidas em âmbito privado.

É nesse cenário que as redes sociais se integram, uma vez que comportam tendências, preferências e estilos de bilhões de pessoas no mundo a partir do compartilhamento de informações, opiniões, dados particulares e grupos de interesse. Todavia, essa experiência pode acarretar em abusos e invasões de direitos fundamentais do usuário, tais como intimidade, privacidade e liberdade, resumindo-o a mero instrumento que produz conteúdo para redes processadoras de dados que podem utilizá-los ilimitadamente, violando seus direitos em favor do interesse empresarial/mercadológico.

Diante dessa realidade, em novembro de 2010, o Ministério da Justiça buscou amparo na contribuição popular, por meio de uma consulta pública, sobre o primeiro anteprojeto de lei de proteção de dados pessoais. Concluída seis meses depois, as proposições apresentadas dão ensejo ao Projeto de Lei 4.060/2012, apresentado na Câmara dos Deputados.

Um ano depois, em 2013, o mundo toma conhecimento das informações divulgadas por Edward Snowden acerca dos dados obtidos por uma agência americana mediante espionagem

de governos, políticos, dados privados contidos em aparelhos telefônicos e eletrônicos, etc. No Brasil, o escândalo acelerou a elaboração de diversos projetos legislativos, bem como suscitou a instauração de uma Comissão Parlamentar de Inquérito da Espionagem no Senado Federal, tendo em vista os dados obtidos pela Agência de Segurança Nacional Americana sobre autoridades nacionais.

Essa CPI inspirou a proposição do Projeto de Lei do Senado nº 131/2014, disposto a regular o fornecimento de dados de cidadãos e empresas brasileiras a organismos estrangeiros. Concomitantemente, era debatido o Projeto de Lei do Senado nº 330/2013, que dispunha sobre a proteção, o tratamento e o uso de dados pessoais. No entanto, em maio de 2014, é promulgada a Lei 12.965, do Marco Civil da Internet, no intuito de estabelecer princípios, direitos e deveres quanto ao uso da internet no Brasil, fator que reduziu o envolvimento político em torno de uma regulação do uso de dados pessoais.

Ainda assim, em 2015 é aberta nova consulta pública, nos moldes da realizada em 2010, de modo que a aquela conta com um nível mais qualificado de discussão e participação popular, tanto que em 2016 seu texto é encaminhado à Câmara dos Deputados, onde se transformaria no PL 5276/2016.

É formada a Comissão Especial que analisaria este Projeto de Lei e o de nº 4.060/2012. Em pouco mais de oito meses, a Comissão realiza 11 audiências públicas que contam com o engajamento de mais de 40 entidades nacionais e internacionais, com fito de aprimorar e equilibrar a redação do texto final à realidade vivenciada pelo usuário na rede.

Um dos pontos positivos para a elogiada redação da Lei Geral de Proteção de Dados foi o envolvimento de representantes de diferentes espectros e partidos políticos, o que facilitou o consenso acerca do conteúdo da lei e a harmonização dos projetos outrora apresentados, resultando na aprovação do PLS 330/2013, pelo Senador Ricardo Ferraço, em outubro de 2017. Outros pontos a favor foram certos acontecimentos em sede internacional que fortaleceram, ainda mais, o debate nacional sobre a necessidade de uma normatização aos moldes da LGPD.

Em primeiro lugar, puderam ser avaliados os riscos políticos da ausência de regulamentação do uso de dados pessoais com as polêmicas envolvendo a empresa

Cambridge Analytica, suspeita de aplicar informações privadas fornecidas por usuários de redes sociais para fins eleitorais, notadamente o suposto favorecimento à eleição de Donald Trump, nos Estados Unidos e a saída do Reino Unido da União Europeia. Os reflexos foram percebidos no Brasil ano passado, durante as eleições, a ponto de o Ministério Público abrir uma investigação para averiguar eventual captação ilícita de dados pessoais de maneira não autorizada por campanhas políticas.

Em outro giro, o Brasil se sentiu motivado em desenvolver a LGPD, especialmente após a aprovação do *General Data Protection Regulation*, instrumento normativo criado pela União Europeia, mas de alcance extraterritorial, disposto a conformar a atuação de empresas, processadores de dados e fornecedores de produtos e serviços a normas de proteção à privacidade e intimidade do usuário/consumidor. Para tanto, foram instituídas multas milionárias em desfavor daqueles que descumprirem as normas previstas no GDPR e impostas restrições à atuação comercial no principal bloco econômico do mundo.

O interesse nacional em ingressar na lista de países que compõe a Organização para a Cooperação e Desenvolvimento Econômico – OCDE também motivou os trabalhos em torno da Lei 13.709/18, uma vez que o ente internacional estipula regras de proteção de dados pessoais que devem ser internalizadas por seus componentes, visando conferir segurança jurídica aos cidadãos e formas transparentes de atuação no meio virtual. Nesse sentido, criou-se um grupo de análise de assuntos econômicos no bojo da respectiva comissão do Senado Federal, a qual destacava a importância econômica e estrutural para o país do avanço da LGPD, já que ela propiciaria o incremento das relações comerciais e o aumento do investimento internacional no país.

Considerados esses fatores, em 2018, o Senado Federal aprovaria o PLC 53/2018, que geraria a Lei 13.709/18, a qual contaria com significativo apoio das casas do Congresso Nacional devido à unanimidade dos membros quanto à aprovação da redação final, ao mesmo tempo em que possibilitava ao Brasil avançar econômica e socialmente em um cenário cada vez mais delicado e essencial para o Estado Democrático de Direito: a proteção dos direitos fundamentais relacionados à divulgação de dados pessoais na internet e seu respectivo uso.

2. ANÁLISE DO CONSENTIMENTO À LUZ DO PRINCÍPIO DA AUTODETERMINAÇÃO INFORMACIONAL

Nos últimos anos, as inovações tecnológicas estão em constante diversificação, com utilização de mecanismos cada vez mais sofisticados e, ao mesmo tempo, potencialmente nocivos à tutela da privacidade. Nessa toada, o dinamismo oferecido não comporta regulação por meio de normativas que mais engessam a evolução do que necessariamente protejam os usuários, devendo haver um equilíbrio entre os dois lados sob o risco de haver violação ao livre desenvolvimento da personalidade.

Considerando a necessidade em resguardar a proteção de dados pessoais como um novo direito da personalidade, é necessário haver uma "redefinição do conceito de privacidade que, além do tradicional poder de exclusão, atribui relevância cada vez mais ampla e clara ao poder de controle"[42]. Trata-se da chamada autodeterminação informativa, entendida como a capacidade do indivíduo em controlar suas próprias informações, desde a "obtenção, titularidade, tratamento e transmissão de dados relativos a ele"[43].

Esse conceito não é novo no ordenamento jurídico, já tendo servido de embasamento em alguns julgados que versam sobre dados, como objeto no voto do Ministro Luiz Fux, em sede do Recurso Extraordinário nº 673707 / MG[44], acerca do reconhecimento do habeas data como garantia constitucional adequada para a obtenção, pelo próprio contribuinte, dos dados concernentes ao pagamento de tributos constantes de sistemas informatizados de apoio à arrecadação dos órgãos da administração fazendária dos entes estatais. *In verbis*:

> "Assegurando a Lei Maior ao impetrante contribuinte o direito de conhecer as informações e anotações que lhe digam respeito, deve-se entender como possível a impetração do habeas data de forma a esclarecer à pessoa jurídica ou física os valores por ela pagos a título de tributos ou qualquer outro tipo de pagamentos constantes dos registros da Receita Federal Brasil ou qualquer outro órgão de Administração Fazendária das outras entidades estatais."

---

[42] RODOTÀ, Stefano. **A vida na sociedade de vigilância - a privacidade hoje.** Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro. Renovar, 2008.

[43] TEFFÉ, Chiara Spadaccini de. Consentimento e Proteção de Dados Pessoais na LGPD. In: TEPEDINO, G. (Coord.); Frazão, A. (Coord.); OLIVA, M. Milena (Coord.). **Lei Geral de proteção de dados pessoais e suas repercussões no Direito Brasileiro**. Revista dos Tribunais, 2019.

[44] BRASIL. Superior Tribunal Federal. Recurso Extraordinário nº 673707/MG. Habeas Data. Recorrente: José Roberto Roca Guimarães e outros. Recorrido: União. Relator: Ministro Luiz Fux. Brasília, 17 de junho de 2015.

Assim, as mídias sociais devem ser moldadas de forma a instrumentalizar essa capacidade do usuário, empoderando-o de forma que ele possa operacionalizar suas decisões e garanti-las, uma vez que dependem de ações próprias. E, nesse sentido, o consentimento é tido como o seu vetor central, visto que, por meio dele, são fornecidas múltiplas autorizações para a plataforma.

2.1. Requisitos para a obtenção do consentimento válido.

Inicialmente, cabe ressaltar que, para que seja possível a utilização de uma rede social, é necessário que o usuário aceite as cláusulas contidas nos termos e condições de uso expostos pela plataforma. As diretrizes e regulamentações ali contidas, nada mais são do que as disposições contratuais de um negócio jurídico estabelecido entre o usuário e a plataforma.

Nesse sentido, a aceitação é o ato de concordância com o instrumento contratual estabelecido, que se dá, via de regra, pela assinatura das partes em tal documento. Ocorre que no mundo digital, essa anuência costuma ser dada, na maioria das vezes, pelo simples *check* em uma caixa que assinala a leitura e concordância com os termos e condições de uso disponibilizados. E como garantir que, dessa forma, o consentimento dado pelo usuário foi válido?

Antes de responder tal questionamento, é necessário conceituarmos o instituto do consentimento.

No Regulamento Geral sobre a Proteção de Dados (GDPR, na sigla em inglês), o consentimento é definido como "uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento” [45].

Já na Lei Geral de Proteção de Dados, legislação brasileira sobre a temática, também se compreende o consentimento como uma "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade

[45] Art. 4º, 11, **General Data Protection Regulation (GDPR)**. Acesso em: 12 de agosto de 2019.

determinada”[46].

Assim, conforme explicitado acima e considerando o conceito trazido pela legislação brasileira, para que o consentimento seja considerado válido, ele deve preencher alguns requisitos, expostos individualmente a seguir. Ressalta-se que, numa leitura do ordenamento jurídico como um todo, é vedado o tratamento de dados nas hipóteses de vício do consentimento, previstas no Código Civil.

2.1.1. Livremente dado.

Apesar da subjetividade do termo, o seu objetivo é garantir ao indivíduo o direito de escolha quanto aos dados sobre os quais ele gostaria de dispor.

De acordo com Bruno Bioni[47], para que o consentimento seja considerado livre, o usuário deve possuir o poder de fornecê-lo para diferentes funcionalidades destacadas individualmente, numa espécie de consentimento fatiado:

> "A questão central é sempre checar a existência de algum tipo de subordinação - assimetria de poder - que possa minar a voluntariedade do consentimento, devendo haver uma analise casuística para se concluir se o consentimento pode ser adjetivado ou não como livre."

Nos casos em que se exige o consentimento como condição para a utilização do serviço, sem oferecer ao usuário mecanismos de controle sobre as informações oferecidas, cabe a plataforma comprovar como isso indica que o consentimento foi dado livremente.

Isso se aplica também aos provedores que obtém o consentimento de forma omissiva, por meio do qual a mera abstenção do usuário expressa a sua concordância com as previsões expostas, como, por exemplo, nos casos em que continuidade da navegação em um site significa a sua total anuência. Nessa forma de consecução, o usuário forneceria uma espécie de "cheque em branco" para a coleta e tratamento desses dados, o que viola toda a política de proteção.

---

[46] Art. 5º, XII, **Lei Geral de Proteção de Dados (LGPD)**. Acesso em: 12 de agosto de 2019.
[47] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e o limite do consentimento. Rio de Janeiro: Forense, 2019.

A forma mais adequada, já aplicada por alguns provedores, é a disponibilização individualizada de caixas *opt in*[48] para que o usuário possa concordar ou discordar isoladamente com o tratamento de dados para as diferentes finalidades.

Nesse sentido, como forma de garantir a liberdade de escolha e os meios de proteção ao usuário, a LGPD prevê que, "quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 da Lei.[49],,[50].

2.1.2. Informado.

Tal adjetivação do consentimento relaciona-se ao princípio da finalidade[51], por meio do qual a realização do tratamento deverá observar os propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

A expressão tem o claro condão de assegurar ao usuário a compreensão genuína de quais dados serão coletados, como será realizado o seu tratamento ou qual o propósito para o seu uso, para que assim as organizações certifiquem-se que estão claramente explicitando o que deverá consentido.

Tal adjetivação do consentimento busca fornecer ao usuário mecanismos de autoproteção, bem com dar efetividade à autodeterminação informacional. A plataforma deve, portanto, oferecer mecanismos para conferir transparência ao fluxo dos dados.

Dessa forma, incluir informações com vocabulário denso na política de privacidade, assim como ocultá-las, dificultando o seu acesso e compreensão por meio de textos com letras pequenas, são condutas que vão de encontro do necessário para se estabelecer o consentimento informado.

---

[48] *Opt-in* significa a expressão da vontade de um usuário de internet, afastando-se sua presunção de aceite pelo silêncio. Será tratado com mais profundidade no item 1.3.2. deste trabalho.
[49] O artigo 18 da LGPD trata dos direitos do titular dos dados pessoais, como o de acesso e correção.
[50] Art. 9, § 3º, **Lei Geral de Proteção de Dados (LGPD)**. Acesso em: 12 de agosto de 2019.
[51] Art. 6º, I, **General Data Protection Regulation (GDPR)**. Acesso em: 12 de agosto de 2019

2.1.3. Inequívoco.

Essa característica se assemelha muito ao dever de informar, acima exposto. Ressalta-se a sua relação com o princípio da finalidade também, uma vez que o consentimento só pode ser dado para um determinado direcionamento, não cabendo exposições genéricas que tenham como objetivo induzir o indivíduo a concordar com o tratamento de dados realizado.

Conforme exposto por Bruno Bioni[52],

> "Os adjetivos informado e livre são calibrados pela locução 'finalidades determinadas'", uma vez que a definição de uma finalidade é o que permitirá analisar regressivamente se o cidadão foi adequadamente informado para iniciar um processo de tomada de decisão livre".

2.1.4. Específico.

A LGPD, diferente da GDPR, da Lei do Cadastro Positivo e do Marco Civil da Internet, que utilizaram o vocábulo "expresso" no seu texto, preferiu o termo "específico" para referir-se aos dados pessoais que merecem uma atenção especial do legislador, devido ao risco que possui o seu tratamento. São eles: por controladores diferentes, sendo que apenas um obteve a anuência do titular[53]; para o tratamento de dados sensíveis[54]; para o tratamento de dados pessoais de crianças e de adolescentes [55]; no caso de transferência internacional de dados para outro país com proteção menor que a do Brasil[56].

A problemática na utilização do termo "específico" ao invés do termo "expresso" está na falta de clareza e redundância, isso porque, conforme exposto por Bruno Bioni[57]:

> "O consentimento já deve ser necessariamente direcionado para propósitos 'específicos e explícitos' na linha do que dispõe princípio da finalidade. Essa significação já está contida na própria definição de uma declaração de vontade que deve ser dirigida para 'finalidades determinadas'.

---

[52] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e o limite do consentimento. Rio de Janeiro: Forense, 2019.
[53] Art. 7º, §5°, **Lei Geral de Proteção de Dados (LGPD)**. Acesso em: 13 de agosto de 2019.
[54] Art. 11, I, **Lei Geral de Proteção de Dados (LGPD).** Acesso em: 13 de agosto de 2019.
[55] Art. 14, §1°, **Lei Geral de Proteção de Dados (LGPD)**. Acesso em: 13 de agosto de 2019.
[56] Art. 33, VIII, **Lei Geral de Proteção de Dados (LGPD)**. Acesso em: 13 de agosto de 2019.
[57] BIONI, op. cit.

> Diante desse cenário, o desafio interpretativo é extrair qual seria a camada adicional de proteção conferida por esse consentimento especial, ainda que o seu qualificador não seja singular do ponto de vista de uma interpretação sistemática da LGPD. Parece-nos que a saída é enxergá-lo como um vetor para que haja mais assertividade do titular com relação a esses movimentos 'específicos' de seus dados."

Entretanto, isso não impede a legislação em conferir aplicabilidade quando o assunto é fornecer maior proteção ao seu usuário, devendo a plataforma, portanto, obter um duplo grau de proteção para as hipóteses que envolvem o tratamento dos dados dessa categoria.

2.2. Formas de obtenção do consentimento.

Esgotado o tópico acima, observa-se que progresso geracional das leis de proteção de dados pessoais preocupou-se mais com a adjetivação do consentimento do que com a operacionalização dele, o que abriu margem para que as empresas estabelecessem suas próprias regulações, como os termos e condições de uso dos provedores. Por conseguinte, as previsões pouco se importam com a garantia de controle do usuário sobre as suas informações, esvaziando o real sentido da concordância e autorização fornecida.

Nesse sentido, estudaremos, a seguir, as formas mais utilizadas pelas plataformas para obter o consentimento do usuário, bem como as implicações acarretadas em matéria de validade e proteção.

2.2.1. Consentimento implícito.

Existem circunstâncias nas quais a anuência do usuário não precisa ser explícita, uma vez que o propósito do uso dos dados é transparecido de maneira bem específica e óbvia aos seus olhos. Entretanto, isso não dispensa a necessidade de uma ação positiva do indivíduo, seja por meio do fornecimento de informações ou, até mesmo, de acesso a conteúdos.

Para que a explicação seja mais bem compreendida, podemos citar como exemplo, sites que se utilizam de *cookies* para armazenar as informações sobre o que você faz na Internet. Por meio de um notório e grande aviso, eles informam que, para o acesso, é obrigatória a sua concordância com a política. Quando o indivíduo, após ler o aviso, concorda e continua sua navegação na plataforma, estamos diante do consentimento implícito.

Tal tipo de consentimento, além da ação positiva do usuário, precisa preencher necessariamente os requisitos da obviedade e publicidade para ser considerado válido. Não poderá ser considerado implícito quando o anúncio for de difícil percepção e compreensão, portanto.

Apesar da clareza na transmissão da informação, entendemos que ela não seria o suficiente para ser compreendida como um mecanismo de consentimento, visto que é necessário que o indivíduo entenda perfeitamente e conscientemente o que ele está compartilhando.

2.2.2. Caixas “opt-in" e “opt-out”.

Inicialmente, cabe explicar que caixas *opt-in* referem-se aos locais em que o usuário assinala indicando que concorda com a política de uso, privacidade ou de cookies, bem como o recebimento de informações no seu endereço eletrônico. Entende-se que essa forma requer uma ação positiva, conferindo um consentimento claro e específico.

Já as caixas *opt-out* são opostas. Nelas, é necessária uma ação positiva do usuário também, no entanto, ele deve marcar para explicitar que não concorda com o recebimento de mensagens de marketing, por exemplo.

Ressalta-se que, mesmo essa forma de obtenção sendo predominante na maioria das redes sociais acessadas pela sociedade, elas não podem ser totalmente confiáveis, uma vez que não é possível assimilar se, de fato, aquele consentimento foi dado de maneira consciente pelo usuário e, até mesmo, se foi o próprio quem consentiu.

Em decisão acerca da temática, a Autoridade Espanhola de Proteção de Dados multou a companhia aérea Vueling Airlines em 30.000 euros pelo não por fornecimento de um mecanismo adequado de aviso de *cookies,* estando em desconformidade com o Regulamento Geral de Proteção de Dados da União Europeia - GPDR.

A decisão foi baseada no fato da publicidade utilizada exibir informações genéricas sobre o intuito dos *cookies* e funcionamento, oferecendo como opção ao usuário apenas

aceitar ou rejeitar por padrão todos eles, sem que houvesse o fornecimento de um sistema de gerenciamento granular, que permitiria ao usuário compreender de forma mais detalhada a sua função.

2.3. Consequências da negativa do usuário em fornecer o consentimento

Conforme tratado no início desse capítulo, o mero aceite nos termos e condições de uso da plataforma não implica num grau satisfatório de garantia da autodeterminação informacional do usuário que caracterize o efetivo consentimento. Levando essa realidade em conta, o legislador estipulou no art. 18º, da LGPD, direitos para exercício do titular em relação aos seus dados tratados pelo controlador, podendo ser requisitados a qualquer momento.

É importante ressaltar que mesmo com o direcionamento dos direitos do titular ao controlador, isso não obsta a sua persecução contra operadores e encarregados. Ainda que o legislador tenha especificado o agente, ele não quis restringir o campo de atuação, devendo ser compreendido como oponíveis a todos os envolvidos nas atividades de tratamento de dados, em consonância com o disposto no art. 5º, da LGPD.

Dentre as hipóteses previstas, temos o direito de confirmação do tratamento, de acesso, correção, anonimização, portabilidade, bloqueio, revogação do consentimento e da eliminação dos dados.

Com relação à revogação, com previsões nos arts. 8º, §§ 5º e 6º e 9º, § 2º, da LGPD, o titular tem o direito de revogar o consentimento a qualquer tempo mediante manifestação expressa, por procedimento gratuito e facilitado, bem como nos casos em que haja discordância com as alterações quanto ao tratamento de dados. Em linhas simples, revogar o consenimento deve ser tão simples quanto fornecê-lo.

Já o direito à eliminação de dados, disposto nos incisos IV e VI, do art. 18º, da LGPD, tem duas hipóteses de ocorrência: a primeira refere-se aos casos em que houver dados desnecessários, excessivos ou tratados em desconformidade com a Lei; a segunda concerne aos dados tratados com o consentimento do titular.

A diferença crucial entre a revogação e a eliminação está na retroatividade das duas medidas. Quando solicitada a revogação, os dados tratados sob amparo do consentimento serão ratificados, passando a vigorar os seus efeitos a partir da solicitação. Nos casos de eliminação, todo o tratamento ocorrido com os dados do titular será excluído, exceto nas hipóteses previstas no art. 16, da LGPD.

Cabe frisar, portanto, as finalidades para as quais os dados serão conservados, mesmo diante do requerimento de eliminação ou do término do tratamento. São os casos de cumprimento de obrigação legal ou regulatória pelo controlador; estudo por órgão de pesquisa, garantida a anonimização nos casos em que for possível; transferência a terceiro; ou uso exclusivo do controlador, anonimizado e vedado acesso por terceiro.

Em uma análise prática, seriam as hipóteses de armazenamento de dados para fins de *compliance* em uma empresa; retenção de dados de consumo, como notas fiscais, para apresentação ao Fisco; guarda obrigatória de registros, como de determinadas informações de *log in*, conforme explicitado no Marco Civil da Internet[58]; dentre outros.

Ademais, nas outras situações em que a base legal do tratamento de dados não for o consentimento, o titular de dados que se opor a ele, deverá comprovar o descumprimento da Lei, conforme §2º do art. 18, LGPD. Trata-se de uma medida a mais na qual o titular precisará atuar caso esteja em desacordo com a manipulação dos seus dados, devendo haver, então, uma comunicação motivada por ele.

Com relação ao direito de revogação do titular, o Serviço de Proteção de Dados Pessoais da Polônia impôs, recentemente, uma multa administrativa de mais de 201.000 PLN (moeda polonesa)[59] à empresa ClickQuickNow pela obstrução no exercício do direito de retirada do consentimento para o tratamento de dados pessoais. De acordo com a autoridade, a empresa não levou em consideração que a retirada do consentimento deveria ser tão fácil quanto o seu fornecimento – pelo contrário, aplicou soluções organizacionais e técnicas complicadas em relação à sua retirada.

[58] Art. 7º, inciso X, Lei 12.965, de 23 de abril de 2014 (Marco Civil da Internet).
[59] ZSPR.421.7.2019. Personal Data Protection Office. Varsóvia, 16 de outubro de 2019. Disponível em: https://uodo.gov.pl/decyzje/ZSPR.421.7.2019. Acesso em: 14 de novembro de 2019.

Nessa toada, uma problemática seria a escolha por empresas em arcar com as multas impostas ao invés de fornecer mecanismos mais efetivos de retirada do consentimento e eliminação de dados, uma vez que a sua exploração mercadológica pode ser muito mais interessante e rentável.

Paralelamente, independente do requisito legal utilizado como base pelo controlador, a legislação estipulou outra exceção para legitimar a manutenção do tratamento de dados, mesmo nos casos de revogação pelo titular. Vejamos o inciso III, do art. 15, da LGPD, *in verbis*:

> "Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses: [...]
> III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público".

Levando em consideração o disposto na legislação, temos a figura do interesse público, o qual permite ao controlador o tratamento dos dados mesmo que o titular o tenha revogado ou eliminado. Mas, o que de fato seria esse interesse público? A mesma terminologia aparece outras vezes no texto da Lei[60], todavia, o legislador não estipulou o seu conceito, tratando-se, portanto, de um termo aberto.

No que diz respeito aos outros momentos em que o termo se encontra presente, temos sua correlação com aspectos em torno do tratamento de dados pessoais pelas pessoas jurídicas de direito público, bem como ao tratamento daqueles dados cujo acesso é público, entendendo que em tais situações deve haver atendimento ao interesse público.

Ocorre que, tal generalização quanto à vinculação ao "interesse público" abre margem para uma interpretação extensiva que permitiria o compartilhamento dos dados em nome da eficiência da administração pública e de uma segurança pública.

Nesse sentido, o interesse público deve ser compreendido, em uma leitura do ordenamento jurídico, como o sinônimo de interesse coletivo, nacional, no qual os anseios sociais se sobreporiam aos particulares.

---

[60] Art. 4º, §1º ; art. 17, §3º; e art. 23, caput, **Lei Geral de Proteção de Dados (LGPD)**.

É o caso, por exemplo, do Portal da Transparência, um site de acesso livre, no qual o cidadão pode encontrar informações sobre como o dinheiro público é utilizado e sobre a gestão pública do Brasil, o que incluem dados acerca do pagamento de servidores.

Em 2015, em ação proposta por uma servidora inconformada com a divulgação de seus dados, o STF, por decisão unânime no julgamento do Recurso Extraordinário com Agravo nº 65777/SP [61], entendeu que a divulgação oficial da remuneração de servidores públicos com o nome dos respectivos titulares é de interesse geral e não viola o direito à intimidade e à privacidade. Para o Tribunal, a pessoa que decide ingressar no serviço público adere ao regime jurídico próprio da Administração Pública, que prevê a publicidade de todas as informações de interesse da coletividade:

> "Sua remuneração bruta, cargos e funções por eles titularizados, órgãos de sua formal lotação, tudo é constitutivo de informação de **interesse coletivo** ou geral. Expondo-se, portanto, a divulgação oficial. Sem que a intimidade deles, vida privada e segurança pessoal e familiar se encaixem nas exceções de que trata a parte derradeira do mesmo dispositivo constitucional (inciso XXXIII do art. 5º), pois o fato é que não estão em jogo nem a segurança do Estado nem do conjunto da sociedade." [grifo nosso].

Uma exemplificação que se relaciona ao interesse público, numa análise comparativa com a GDPR, foi o parecer [62] emitido pela Comissão Nacional de Proteção de Dados, autoridade nacional de Portugal, a pedido da Entidade Reguladora da Saúde (ERS), sobre a recusa de prestação de serviço por parte de unidades de saúde a titulares de dados que não assinaram declaração de autorização de tratamentos dos seus dados pessoais.

De acordo com a autoridade, o consentimento não é a condição adequada para legitimar os tratamentos de dados pessoais necessários à prestação de cuidados de saúde. Isso porque, uma vez sendo essenciais para a realização do serviço, não há margem para o seu fornecimento ou não. Eventual recusa pelo paciente em assinar um formulário de outorga de consentimento simplesmente inviabilizaria a realização do exame.

---

[61] BRASIL. Superior Tribunal Federal. Agravo em Recurso Extraordinário nº 65777/SP. Garantias Constitucionais. Proteção da Intimidade e Sigilo de Dado. Recorrente: Município de São Paulo. Recorrido: Ana Maria Anbreu Lacambra. Relator: Ministro Teori Zavaskci. Brasília, 23 de abril de 2015.
[62] PORTUGAL. Comissão Nacional de Protecção de Dados. Parecer n.º 25/2019, de 10 de maio de 2019.

Os referidos casos concretos corroboram a afirmativa de que o consentimento não é a principal base legal prevista nas legislações que versam sobre proteção de dados pessoais, tampouco está hierarquiamente acima das demais. Cada uma das bases legais que legitimam o tratamento de dados pessoais tem sua particular importância e são mais ou menos adequadas para tutelar situações fáticas.

De todo o modo, o interesse público não oderecer permissibilidade à violações que ultrapassem a sua esfera de atuação, sob o pretexto, por exemplo, de melhoras, principalmente na segurança pública, que perceptivelmente vem conduzindo à uma relativização da proteção de dados, vide a utilização de reconhecimento facial pelas polícias brasileiras[63].

[63] SISTEMA de reconhecimento facial da PM do RJ falha, e mulher é detida por engano. **Portal de Notícias G1**, 2019. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml. Acesso em: 14 de novembro de 2019.

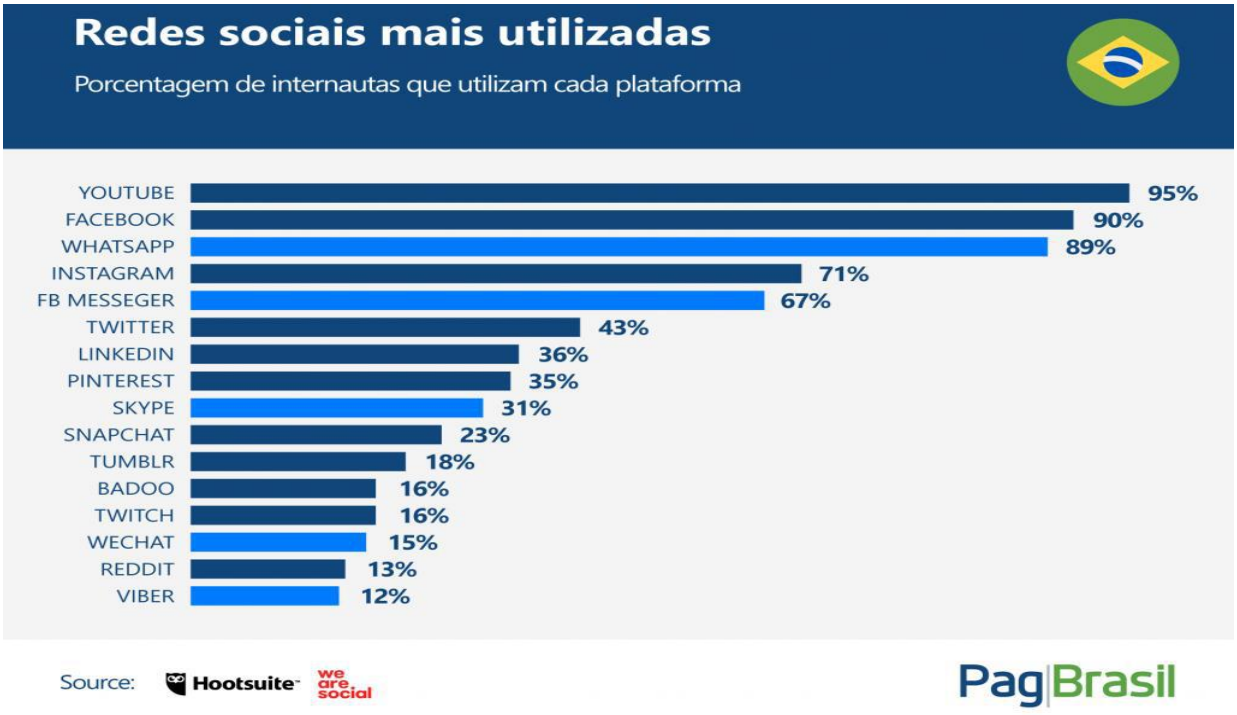
3. ESTUDO DE CASO

Neste capítulo, tendo em vista a abordagem ao longo deste trabalho sobre as mudanças advindas com a intensificação do uso da Internet e, principalmente, das redes sociais, bem como da necessidade que isso impôs ao debate acerca da proteção de dados pessoais, analisaremos com mais detalhes o que efetivamente significa concordar com os termos e condições de uso quando você se cadastra em uma delas.

Foram escolhidas como material de análise as redes sociais mais populares do país, cada uma com suas funções específicas de acordo com o público que se propõe a alcançar, seja no entretenimento, na informação ou, até mesmo, na busca pelo aperfeiçoamento profissional. Consequentemente, existiram peculiaridades sobre as formas de coleta e uso dos dados fornecidos pelos usuários, uma vez que são voltadas para diferentes finalidades.

Nesse sentido, foram buscadas e analisadas as políticas de privacidade e os termos de uso do Facebook, Instagram, Twitter e Linkedin, selecionadas pelo critério de impacto e relevância social que possuem no cenário atual, conforme demonstrado por meio do gráfico contido na figura 2.

Figura 2 – Redes sociais mais utilizadas.



Fonte: We Are Social e Hootsuite.

Considerando o tempo médio de 2 minutos para leitura de cada página realizada, foram gastos para a realização desse capítulo um total de 4 horas e 32 minutos para uma compreensão básica, sem adentrar em detalhes ou tecer qualquer tipo de observação. Essa informação demonstra o tempo médio que cada usuário abdicaria apenas para ler as condições antes de criar uma conta em tais plataformas. O que demonstra certa incompatibilidade entre a dinamicidade oferecida pela rede e a necessidade de uma leitura densa para saber ao que está se submetendo.

A seguir, serão esmiuçados individualmente os conteúdos encontrados.

3.1. Facebook

Se você não tem uma conta no Facebook, certamente sua existência é colocada em questionamento no mundo. Isso porque, nos últimos dez anos, a sua utilização popularizou-se exponencialmente por um público bem diversificado, que inclui diversas faixas etárias, personalidades e opiniões políticas.

O Facebook tem como marca o fato de ser uma rede social versátil e abrangente, que reúne multi-funcionalidades em uma mesma plataforma. Serve tanto para gerar negócios quanto para conhecer pessoas, relacionar-se com amigos, família e manter-se informado sobre os acontecimentos no mundo.

Seu surgimento se deu numa tentativa de concorrência com o *Orkut, até então* hegemônico na função de site de relacionamento mais utilizado no país. Desde então, tal rede social conquistou posição de destaque, tornando-se a maior no planeta, com uma marca que ultrapassa os 2,2 bilhões de usuários.

Tendo em vista a grandeza da sua perfomance, questiona-se como a empresa consegue ganhar tanto dinheiro se a utilização é gratuita? Essa dúvida possui uma resposta muito simples: o produto é o usuário.

Estima-se que, aproximadamente 89% do faturamento do Facebook é proveniente de anúncios digitais. Ou seja, as empresas pagam ao Facebook para o usuário da rede social veja os produtos que elas estão vendendo. Em 2018, o Facebook teve uma receita total de US$ 55

bilhões (cerca de R$ 204 bilhões). Atualmente, pode-se dizer que todas as grandes marcas do mercado estão ativas no Facebook e no Instagram, que pertence ao mesmo grupo.

A publicidade está por toda parte dentro da rede social, em banners, posts e stories, em formato de textos, fotos, GIFs e vídeos. O pagamento, geralmente, é feito por cada clique dos usuários nos anúncios. Outra fonte de renda seriam os anúncios segmentados, que se utilizam de dados pessoais e demográficos captados pelo Facebook para atingir um público específico.

Nesse sentido, o gerenciamento dos dados pessoais presentes nessa plataforma merece uma atenção especial, visto que engloba informações consideráveis de uma parcela bastante expressiva da população. Nessa toada, por conta dos últimos escândalos de vazamento envolvendo-a, a análise dos seus termos e condições de uso é fundamental.

Assim, para a elaboração deste trabalho, o material base utilizado foram os termos de serviço, a política de cookies e a política de dados do Facebook.

Inicialmente, cumpre ressaltar que, quanto aos termos e condições de uso da plataforma, aplica-se a legislação geral sobre dados pessoais no país, uma vez que há operação de tratamento de dados realizada por pessoa jurídica de direito privado, que, independentemente do meio, do país de sua sede ou do país em que estejam localizados os dados, realiza operação de tratamento e coleta de informações de indivíduos localizados em território nacional, além do tratamento ter por objetivo a oferta ou o fornecimento de bens ou serviços no Brasil.

Dito isto, passamos para a análise do conteúdo presente em tais termos. Logo na introdução, a plataforma explicita que o uso não é cobrado e que, em vez disso, a renda é advinda de empresas e organizações que possuem interesses em divulgar seus produtos e serviços. Assim, ao utiliza-lá, você estará concordando em receber anúncios que sejam considerados de seu interesse com base nos seus dados pessoais, usados para ajudar a determinar o que deve ser mostrado.

Ocorre que, esses anúncios, de acordo com o exposto, podem ser mostrados dentro e fora dos produtos das Empresas do Facebook. O questionamento é quanto à extensão dessa publicidade fora, já que não foram detalhadas as condições sobre as quais ela ocorre, apenas restringindo-se a dizer que todas as informações utilizadas são fornecidas pelo Facebook.

Além disso, também é dada pelo usuário a permissão para utilizar o seu nome, foto do perfil e informações para ações com anúncios e conteúdo patrocinado, ou seja, uma forma de propaganda para os anunciantes com a utilização dos seus dados, sem que haja qualquer tipo de remuneração por isso. É o que acontece, por exemplo, quando o seu nome aparece para os amigos da rede dentre aqueles que curtiram o conteúdo de uma página comercial visitada.

Quanto aos dados partilhamos e informações de identificação pessoal, o Facebook ressalta que eles não são vendidos para anunciantes e nem compartilhados, a menos que seja dada uma permissão específica. Todavia, a forma como essa permissão deveria ser dada não é explicitado, o que abre uma margem negativa para o usuário.

Nesse sentido, a rede expõe que os anunciantes não possuem capacidade de identificar ou escolher diretamente o alvo de suas propagandas, uma vez são aceitos apenas filtros que informem suas metas comerciais e o tipo de público que desejam alcançar com o anúncio.

Isso ocorre porque o Facebook utiliza-se de dados anonimizados, ou seja, aqueles relativos a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do seu tratamento, conforme redação do art. 5º, III, da Lei 13.709/2018.

Assim, necessária seria a obtenção de um novo consentimento, específico e informado, no qual o usuário concordaria com o fornecimento pelo Facebook de seus dados para anunciantes.

Um ponto positivo é a escrita dinâmica utilizada, que retira o aspecto contratual e facilita a percepção do usuário ao que ele está concordando. Porém, ao longo da leitura, nos deparamos com a utilização de termos que tentam suavizar a real intenção no uso dos dados para a publicidade direcionada, sugerindo ser uma forma de "personalizar sua experiência", "ajudar a encontrar entidades de interesse nos Produtos do Facebook" ou "criar produtos personalizados que sejam únicos e relevantes para você".

Nos serviços fornecidos pelo Facebook para combater condutas prejudiciais, proteger e oferecer suporte para a comunidade, a plataforma estabelece a possibilidade de

compartilhamento de dados com outras Empresas do Facebook quando detectados o uso inadequado ou conduta prejudicial por parte de alguém que esteja usando um dos produtos.

Acontece que, tal previsão não especifica o que seria essa conduta ou uso inadequado e, principalmente, o intuito em fornecer essas informações a outras empresas. Surge a dúvida se seria necessário obter um novo consentimento do usuário ou se a própria concordância com os termos expostos o sujeitaria a isso.

Outra previsão que merece destaque é a interconectividade presente entre Instagram, Messenger e Facebook, justificada como uma forma de fornecer experiências consistentes e contínuas entre as empresas. Assim, ao concordar com os termos de uma delas, você se sujeita ao compartilhamento de informações entre todas, como, por exemplo, aquelas referentes à contatos e conexões.

Dentre as permissões concedidas pelo usuário nos termos de serviço, temos a disposição acerca do armazenamento de fotos. De acordo com a rede social, ao compartilhar uma imagem na plataforma, é cedida permissão para que outras pessoas possam copia-lá e compartilhá-la – dependendo da configuração de perfil escolhida pelo usuário na própria plataforma, que pode ser público ou privado –, bem como os provedores de serviços que fornecem suporte para as outras empresas que compõe o grupo. Essa licença é encerrada quando o conteúdo for excluído dos sistemas do Facebook.

Até aqui, não foi especificado o tempo pelo qual esse dado fica armazenado, visto que não é determinado pelo usuário, e sim, pela plataforma.

Nesse sentido, ao analisar os mecanismos de exclusão dos dados, percebe-se o estabelecimento de um prazo limite de 90 dias para que sejam excluídas definitivamente suas informações, com exceção dos casos previstos em lei, como cumprimento de alguma obrigação legal[64].

No caso de alterações nas disposições dos termos de uso, o usuário será notificado em, no mínimo, 30 dias antes das reformulações, tendo oportunidade de analisar a sua

[64] Art. 16, I, **Lei Geral de Proteção de Dados (LGPD)**. Acesso em: 15 de outubro de 2019.

conveniência antes da entrada em vigor, com exceção dos casos exigidos por lei, no qual não seria necessário o aviso. Caso não concorde com as alterações, o Facebook indica como única alternativa a exclusão da conta.

Na política de dados, dentre as informações e conteúdos fornecidos pelo usuário para a coleta, está a localização de uma foto e, inclusive, o que pode ser visto por meio de alguns recursos fornecidos, como a própria câmera. A plataforma utiliza dessa ação como um mecanismo para oferecer maiores recursos, como sugestão de máscaras e filtros, novamente como uma justificativa para amenizar o acesso ao que enxergamos.

Outras informações coletadas referem-se ao uso da rede social pelo indivíduo, às transações realizadas dentro da plataforma, aos dados fornecidos por outros usuários sobre a sua utilização – fotos marcadas, comentadas ou compartilhadas –, às redes e conexões, bem como elementos acerca do dispositivo utilizado para se conectar.

Com relação às configurações do dispositivo utilizado para acessar a rede, como um *smartphone* ou um *tablet*, afirma que as informações se restringem ao acesso à sua localização GPS, câmera ou fotos. Nesse caso, tais dados são cedidos por meio um consentimento que ultrapassa o limite da plataforma, uma vez que é dado no próprio aparelho que intermediou o acesso. Resta saber se a aceitação é automática com a utilização da rede social, necessitando de uma ação positiva do usuário para desativar tais funções ou se de fato é necessário obter um novo consentimento dele.

Disto isto, no que concerto ao compartilhamento dessas informações coletadas, o Facebook garante que elas são divididas com quem você se comunica – isto é, com o público selecionado para ver suas publicações –, com aplicativos, sites e integrações de terceiros.

Com relação aos itens finais, esses se relacionam aos serviços que utilizam ou estão integrados à plataforma. Por exemplo, a utilização de um jogo ou da interface do Facebook em um site qualquer para comentar ou compartilhar um conteúdo. Essas informações coletadas precisam respeitar termos e políticas próprias, devendo obter o consentimento do usuário para coletar informações que não sejam públicas.

Nesse sentido, o Facebook ressalta que vem restringindo ainda mais o acesso de desenvolvedores aos dados a fim de ajudar a evitar abusos. Como exemplo dessas medidas adotadas, está a remoção do acesso caso o aplicativo terceiro não seja usado por três meses.

Em conformidade com o previsto no art. 18, da Lei 13.709/2018, a rede social garante em seus termos a capacidade de acessar, retificar, portar e apagar os dados. Todavia, com excessão do registro de pesquisa e de cópia de documentação para verificação da conta, o prazo não é estabelecido expressamente para exclusão do conteúdo.

As informações coletadas pelo Facebook podem ser compartilhadas no mundo todo para os fins descritos na politica de dados e acima citados, tanto internamente entre as empresas que compõem o grupo, quanto com parceiros externos. Por meio do aceite nos termos, você consente com a transferência de dados para os Estados Unidos e outros países.

Nesse sentido, temos alguns problemas. A começar, a LGPD[65] prevê a necessidade de um grau de proteção adequado para países ou organismos internacionais que participarão da transferência internacional de dados. Ocorre que, o fato de haver uma previsão genérica nos termos não afasta a responsabilidade do provedor nos casos em que tal norma não for cumprida.

Ademais, a concordância com os termos de uso não pode ser considerado um consentimento específico e em destaque para a transferência, visto que não há distinção clara com outras finalidades.

3.2. Instagram

Tirar fotos, gravar vídeos e compartilhá-los na Internet nunca foi tão usual quanto nos últimos anos, com o advento do aplicativo que revolucionou o mundo da Internet: o Instagram. Difícil sair com amigos e não se deparar com alguém na mesa de um restaurante que sequer provou o prato, mas ansiosamente já garantiu a foto e os likes do dia.

[65] Art. 33, I, **Lei Geral de Proteção de Dados (LGPD)**. Acesso em: 15 de outubro de 2019.

A rede social surgiu em 2010 apenas para os usuários da Apple. Com a possibilidade de adicionar filtros e melhorar o aspecto de fotografias, rapidamente se popularizou, sendo um dos aplicativos mais baixados na Apple Store desde então.

Em 2012, o Instagram teve sua compra anunciada pelo Facebook, em um negócio estimado em US$ 1 bilhão. Desde então, os recursos foram melhorando e, atualmente, a função dos stories vem sendo muito utilizada, uma vez que permite a publicação informal de suas atividades diárias por um período de 24 horas. Tal ferramenta possibilita maior interatividade **e** dinâmica para compartilhar conteúdos na rede.

Aliás, o sucesso é tanto que novas profissões surgiram no mercado de trabalho. Tratam-se dos influenciadores digitais, que nada mais são do que pessoas com milhares de seguidores que perceberam a internet como uma oportunidade de negócio e passaram a ser vistos e valorizados por grandes marcas, graças ao seu alcance por meio de curtidas e comentários.

Com toda a popularidade, a utilização dessa rede também traz o seu ônus. Não é de hoje que se fala no Instagram e um dos temas mais debatidos é a saúde mental. As mudanças efetuadas recentemente na plataforma para esconder a visibilidade das curtidas foram realizadas em função disso. A rede social representa um conjunto de fotos sobre uma realidade virtual impossível: corpos perfeitos, viagens constantes, estilos autênticos e uma vida de sonhos.

Nesse sentido, conforme elucidado acima, percebemos o grau exorbitante de exposição pela qual os usuários estão submetidos, sendo necessária a compreensão das suas políticas para entender o melhor funcionamento da plataforma em matéria de proteção dos dados pessoais.

Assim, como materiais de análise, foram observados os termos de uso, a política de dados e a política de cookies do Instagram.

O conteúdo presente assemelha-se muito ao exposto pelo Facebook, principalmente a política de dados, que é, de fato, a mesma. Para que esse trabalho não se torne redundante, abordaremos apenas os pontos que diferenciam um do outro, uma vez que já expusemos as considerações pertinentes no tópico do Facebook.

De início, temos que, no caso do Instagram, a leitura dos seus termos é mais objetiva e bem menos didática. Suas previsões assemelham-se a um contrato de adesão estabelecido entre duas partes, com a utilização de termos rebuscados e de difícil compreensão para o público leigo. Por exemplo, os seguintes enunciados: “se algum aspecto desse acordo for inexequível, os demais permanecerão em vigor”; “quaisquer alterações ou renúncias relativas a este acordo devem ser feitas por escrito e assinadas por nós”; “se falharmos em executar qualquer aspecto desse contrato, isso não será considerado uma renúncia; “se você for um consumidor, as leis do país em que você reside serão aplicáveis a qualquer pleito, causa de pedir ou disputa que você tiver contra nós decorrente de ou relacionada a estes Termos”.

Além deste, outro ponto que chamou a atenção é referente ao compromisso acordado pelo usuário em permitir o uso do seu nome, da foto do perfil e de informações sobre seus relacionamentos e ações com contas, anúncios e conteúdo patrocinado. O objetivo dessa permissão, de acordado com a plataforma, é obter a interconectividade necessária entre os conteúdos exibidos e pesquisados no Instagram e no Facebook.

Assim, se o usuário possui interesse em um produto do Instagram, o mesmo anúncio aparecerá no Facebook como um conteúdo patrocinado, dando a impressão de que você está sendo ouvido ou, até mesmo, que a sua mente está sendo lida. No entanto, com relação ao uso do microfone, não há previsões que exponham a utilização dessa função para captar anúncios nas plataformas.

Então, como o Facebook parece ouvir o que as pessoas estão dizendo? É que o direcionamento de anúncios é tão preciso que chega a assustar.

Primeiro, o Facebook tem um perfil bastante detalhado sobre os seus interesses, já que vem fornecendo esses dados ao longo dos anos, na forma de curtidas, comentários e cliques. Para ter uma ideia disso, é necessário ir até a página “Suas preferências de anúncios”, dentro das configurações do Facebook, posteriormente, na seção “Suas informações”, e acessar as “Suas categorias”.

A partir disso, é possível analisar que a rede social monitora sua atividade em centenas de milhares de aplicativos e sites que possuem convênios. Com o Facebook Pixel, é possível

rastrear se você fez um cadastro, se adicionou itens ao carrinho, ou até que ponto você leu um artigo. Assim, como explica a própria rede social, é possível "usar esses dados para direcionar anúncios relevantes".

Além disso, a plataforma utiliza-se de informações acerca da localização, conforme já citado, para saber onde você está, seja através do endereço IP, redes Wi-Fi ao redor, ou do GPS do smartphone – nos casos em que essa autorização for dada nas próprias configurações do aparelho. Isso permite às empresas direcionar anúncios com uma precisão enorme.

Nos casos de utilização comercial do Instagram, a responsabilidade por qualquer ocorrência no serviço será limitada ao permitido por lei. Ou seja, nos casos de problemas operacionais, a plataforma resguarda a sua não responsabilidade pelos impactos que poderão ocorrer, como a "perda de lucro, receitas, informação ou dados, ou, ainda, por danos eventuais, especiais, indiretos, exemplares, punitivos ou acidentais". Isso se aplica também aos casos de exclusão do conteúdo, informações ou da própria conta em si.

Com relação ao tempo de remoção de conteúdo e de desativação ou encerramento da conta, a previsão é muito genérica, expondo apenas que poderão permanecer no backup por um prazo limitado, sem especificar que prazo seria esse.

O Instagram determina que, para utilizar os serviços oferecidos, o usuário deve ter pelo menos 13 anos ou a idade mínima legal em seu país. Entretanto, existem contas na rede com milhões de seguidores, conhecidas por toda a comunidade, e que pertencem a crianças com idade menor do que a prevista. A legislação brasileira estipula, no art. 14[66], da LGPD, como

[66] "Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.
§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.
§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.
§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

deve ser o tratamento de dados pessoais de crianças e adolescentes, sendo necessário um consentimento em destaque e específico dado por pelo menos um dos pais para que ele possa ocorrer, conforme previsto no § 1º do artigo citado.

Todas as redes sociais analisadas demonstram não possuir mecanismos compatíveis com a tecnologia disponibilizada de verificação acerca da veracidade das informações dadas por esse público, o que coloca em risco o seu melhor interesse e contraria o disposto no §5º.

Por fim, ressaltamos que a não concordância do usuário com os termos de uso e com as políticas do Instagram implica na impossibilidade de utilização da rede social e, consequentemente, da sua exclusão em um meio digital que é espaço predominante de interações sociais.

3.3. LinkedIn

Atualmente, ser um grande profissional no ramo privado e não ter um perfil no LinkedIn significa fechar portas para novas oportunidades. Isso porque tal rede social tem como função propiciar interatividade entre pessoas e empresas em um meio estritamente voltado para isso.

Assim, através dela, é possível encontrar empregos, novos colaboradores para uma empresa, ampliar o *network*, compartilhar experiências profissionais, fortalecer a credibilidade como profissional e se inteirar sobre o que acontece no mundo dos negócios. Em resumo, ela funciona como uma espécie de currículo virtual.

A diferença do LinkedIn para outras redes sociais, como Facebook, Instagram e Twitter, está justamente no foco dado em conectar profissionais, visto que, mesmo que as outras plataformas permitam tal interação, são muito mais utilizadas para fins de entretenimento.

---

§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.
§ 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança".

E o seu grau de funcionamento caminha de acordo com a quantidade de dados que o usuário fornece à rede. Quanto mais informações forem preenchidas, maior a probabilidade de ser chamado para uma entrevista de emprego. Isso porque o Linkedin serve como um buscador estilo *Google*, ou seja, ele recorre a palavras-chaves exigidas para uma determinada vaga e já elimina candidatos de forma automática.

Hoje, o Brasil é o terceiro país com mais usuários do site, ficando atrás apenas dos Estados Unidos, em primeiro lugar, e da Índia, que ocupa a segunda posição. Nesse sentido, é evidente a importância que essa rede possui no mercado de trabalho brasileiro, devendo ser analisada a forma como ela propõe a tratar os respectivos dados pessoais dos usuários.

Para realização deste trabalho, serviram como materiais de apoio o Contrato do usuário, a Política de *Cookies* e a Política de Privacidade do LinkedIn.

Logo no início do contrato do usuário, a plataforma já expõe a adoção do contrato de adesão no formato do “tudo ou nada”, ou seja, ou o usuário concorda com os termos ali expostos ou não usufrui do serviço. Com a utilização de termos que corroboram com a celebração de um contrato, ao cadastrar-se na rede social, o usuário concorda que está “celebrando um contrato legalmente vinculativo”.

As disposições presentes nos termos vinculam tanto usuários quanto visitantes. Esse modelo evidencia que a concordância não é requisito primordial para que ocorra coleta, uso e compartilhamento de dados, uma vez que o mero acesso já possibilita isso.

Com relação às possíveis alterações no contrato, essas poderão ser feitas a qualquer momento. Em caso de alterações significativas, o usuário será notificado, todavia, o prazo para que ele possa avaliar a pertinência delas não é previsto. No caso de discordâncias, a sugestão dada é o encerramento da conta.

Dente os compromissos estabelecidos pelo usuário, está a necessidade em ter uma "idade mínima", na qual o LinkedIn possa oferecer seus serviços sem precisar do consentimento dos pais ou responsáveis legais. Desta forma, ela é entendida como a idade superior, de acordo com a legislação do país.

Além desse critério, o usuário se compromete a ter somente uma conta, criada com o seu nome verdadeiro, e a não ter sofrido qualquer restrição anterior para utilizar os serviços disponibilizados. Em contrapartida, o LinkedIn se compromete a respeitar as escolhas do usuário no que concerne às configurações de visualização do conteúdo e informações privadas, bem como a oferecer suporte nos casos em que o usuário for, erroneamente, associado a conteúdo de terceiros.

Ainda no contrato do usuário, a rede expõe que o usuário concorda com a autorização de acesso, armazenamento, processamento e utilização de quaisquer informações e dados pessoais fornecidos. O problema de tal assertiva é que a expressão "dados pessoais" engloba uma quantidade imensurável de informação, sendo uma cláusula genérica e que coloca em risco a privacidade do usuário, uma vez que tenta incluir permissões que podem fugir da finalidade inicialmente prevista.

Nessa mesma vertente, no final das disposições que tratam sobre os dados que são coletados na política de privacidade, a plataforma coloca que, tendo em vista que dinâmica os serviços oferecidos necessitam para apresentar novos recursos, talvez seja exigida a coleta de novas informações. Caso sejam coletados dados pessoais substancialmente diferentes ou seja alterada de forma significativa o uso desses dados, o usuário será notificado. Dessa forma, primeiro haverá a coleta e, posteriormente, a obtenção de um novo consentimento, o que não faz sentido sob a ótica da proteção de dados.

Quanto às preferências de anúncios, o LinkedIn adere aos princípios de autorregulamentação em relação à publicidade baseada em interesses e oferece opções para desabilitar tal função. É importante salientar que isso não impede o recebimento de publicidade, apenas restringe o uso da direcionada.

Na política de privacidade são discorridas as opções de acesso e controle do usuário sobre seus dados pessoais. Dentre elas, está a de excluir dados, alterar ou corrigir, limpar ou restringir, além de acessar e levá-los. No caso de exclusão da conta, os dados não serão mais visíveis para terceiros em 24 horas, porém só serão definitivamente excluídos em 30 dias após o encerramento. Mesmo após esse período, as informações que não identificam o indivíduo serão retidas.

E, no que diz respeito à transferência internacional de dados, a rede social informa que processa dentro e fora dos Estados Unidos, podendo ser transferido para países onde as leis sejam menos protetivas do que as do próprio país. Essa disposição viola a Lei 13.709/2018, no seu art. 33, inciso I, uma vez que não é garantido grau adequado de proteção no país de destino.

Dentre as previsões acerca da exclusão da responsabilidade, o LinkedIn tenta isentar-se de garantias de qualquer dano, seja ele indireto, incidental, especial, consequente ou punitivo, estipulando o valor fixo de mil dólares ou cinco vezes a taxa mensal do plano anual, o que for menor. Pelo caráter de adesão, no qual o usuário não tem qualquer influência no conteúdo, tal cláusula é exorbitante, e, portanto, abusiva, não devendo produzir efeitos no país.

A política de privacidade possui informações acerca dos controladores de dados, dependendo de cada localidade. Além disso, informa que realiza coleta e tratamento de dados apenas quando possui base legal para fazer isso, que incluem o consentimento, o contrato e o interesse legítimo da plataforma, requisitos que corroboram com o estabelecido em alguns dos incisos do art. 7º da LGPD[67].

3.4. Twitter

Há treze anos, surgia o Twitter. Assemelhando-se a uma espécie de microblog, funcionava como um meio de comunicação no qual o usuário tinha a liberdade de escrever textos curtos, de até 140 caracteres, bem como, posteriormente, compartilhar imagens e vídeos.

Conhecido por ser um espaço democrático de liberdade de expressão, sua utilização se popularizou rapidamente no mundo, tornando-se uma rede social que funcionava quase como um diário para as pessoas.

Compartilhar desde o que você come até o horário em que dorme é um prato cheio para

[67] "Art. 7º. O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
I - mediante o fornecimento de consentimento pelo titular;
V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;"

quem deseja obter um perfil bem individualizado do usuário. E, por esse motivo, entendemos necessária a análise dos termos que regem o complexo tratamento desses inúmeros dados.

Atualmente, o Twitter é um canal extremamente importante para a propagação de notícias e informações referentes à política, cultura e entretenimento, justamente por esse caráter de garantidor do livre discurso, sendo utilizado pelos maiores veículos de comunicação e pelas maiores personalidades do mundo.

O dinamismo e imediatismo são as marcas da rede social. Imagine a seguinte situação: você está em um engarrafamento, atrasado, sem saber o real motivo. Acessa o twitter, faz uma busca e, rapidamente, encontra o *tweet* de um motorista que acabou de passar pelo acidente que atrapalhou o tráfego, te permitindo mudar a rota e ganhar mais tempo.

Tem, ainda, a ferramenta dos *Trending Topics*, que é uma lista gerada automaticamente por algoritmos que identificam, em tempo real, os assuntos que estão sendo mais falados no Twitter, por meio das palavras mais postadas em todo o mundo, o que facilita a descoberta das notícias mais importantes do momento.

Nenhum outro canal propicia essa rapidez ao indivíduo. Nesse sentido, tendo em vista a importância social de tal rede, foram analisados: os termos de uso, que versa acerca dos serviços ou temáticas específicas que a rede social tem envolvimento direto ou indireto; a política de privacidade, com informações sobre coleta, uso e compartilhamento de dados pessoais; e a política de *cookies.*

Logo na introdução, o Twitter explicita que objetivo principal da sua política de dados é a capacitação do usuário para que ele possa tomar as melhores decisões sobre as informações que compartilha com a rede. Por essa perspectiva, salientamos que a escrita é objetiva e que os termos de uso são bem detalhados, com a devida explicação sobre como cada dado coletado é utilizado pela plataforma e o propósito do seu tratamento.

Por exemplo, as informações de contatos, como endereço de e-mail ou número de telefone, são usadas para autenticar a conta, mantendo-a segura, bem como para prevenir spam, fraude ou abuso. Além dessa finalidade, também é utilizado para direcionar marketing

nos casos em que a legislação do país permitir. No caso, a LGPD prevê, no art. 10, inciso I, a possibilidade do tratamento de dados para apoio e promoção de atividades do controlador, dente as hipóteses de legítimo interesse.

Diferente das outras redes sociais analisadas, o Twitter permite que o usuário não utilize informações verídicas a respeito da sua identidade, podendo ser empregados pseudônimos se assim preferir.

Outra disparidade relaciona-se ao fato da rede social considerar dados pessoais, tais como nome, nome de usuário, foto do perfil e a localização, como partes integrantes de um conjunto de dados públicos. Os *tweets*[68] e os dados que o envolvem, como data, horário, aplicativo e versão, também são assim considerados.

Dessa forma, as listas criadas, as pessoas seguidas, os seus seguidores, os *tweets* curtidos ou aqueles que você deu um *retweet*[69] também são públicos.

Caso o usuário entenda ser excessiva a disponibilidade sobre as quais esses dados estão emersos, o Twitter oferece ferramentas para minimizar a sua publicidade, como a opção de tornar a conta privada. Ocorre que as configurações estão ajustadas, por padrão, em um modelo que todo conteúdo publicado por seus usuários é público a qualquer interessado, sem a necessidade de sequer ter uma conta na rede social. Assim, o acesso e coleta dos dados por terceiros é uma potencial lesão ao direito à privacidade.

Além das informações serem públicas para toda a comunidade do Twitter, elas também são disponibilizadas a sites, aplicativos e outras pessoas para seu uso, em quantidades limitadas gratuitamente e em grande escala quando pagas taxas de licenciamento. De acordo com a plataforma, essa utilização é regida por termos próprios, disponibilizados para leitura apenas em inglês. O usuário brasileiro, portanto, não possui condições de entender o que está sendo feito com os seus dados.

[68] *Tweet* é o nome utilizado para designar as publicações feitas na rede social do Twitter.
[69] *Retweet* é uma nova postagem do *Tweet* de alguém, dando os devidos créditos ao autor.

Os tweets e o conteúdo acessado pelo usuário são utilizados para fazer uma análise comportamental na rede, determinado os tópicos pelos quais o indivíduo receberá publicidade direcionada, amenizado pela política de dados como o "conteúdo relevante para você".

Nesse mesmo propósito, quando o usuário registra sua conta no Twitter com um navegador ou dispositivo, esses são associados ao seu cadastro para finalidades como a personalização do serviço, com o intuito de fornecer conteúdo de acordo com a sua navegação em outros sites. Por exemplo, se forem visitados sites com conteúdo esportivo no computador, poderão ser mostrados anúncios relacionados a esporte.

Em conformidade com os termos, o Twitter ratifica seu compromisso com os princípios que regulamentam a publicidade digital para publicidade comportamental. Nesse sentido, o consumidor tem a faculdade em receber anúncios com base em seus interesses ou não.

Ressalta ainda que, as políticas de anúncios também proíbem que os anunciantes segmentem propagandas com base em categorias consideradas sensíveis, como raça, religião, política, vida sexual ou saúde.

Com relação às comunicações com outros usuários através de mensagens diretas e privadas, as quais o conteúdo não é público, o Twitter armazena e processa as informações relacionadas a elas. Ademais, a rede social garante que elas não são utilizadas para anúncios.

Entretanto, elas podem ser compartilhadas com prestadores de serviços da rede social, como o *Google Analytics*[70], sob a condição de que utilizem seus dados pessoais privados somente em nome da rede social e de acordo com as instruções dela.

As configurações relacionadas à localização podem ser coletadas, usadas e armazenadas, inclusive a sua posição exata atual ou locais onde o Twitter foi utilizado anteriormente, desde que previamente concordado pelo usuário. O intuito desse tratamento, de

[70] "O *Google Analytics* é um sistema gratuito de monitoramento de tráfego que pode ser instalado em qualquer site, loja virtual ou blog. O objetivo principal do Google Analytics não é apenas saber quantos usuários acessam o seu site e sim, de que forma esses usuários se comportam ao navegar pelas diversas páginas e seções deste site." Fonte: Academia do Marketing. Disponível em: https://www.academiadomarketing.com.br/o-que-e-google-analytics/. Acesso em: 31/10/2019.

acordo com a plataforma, é personalizar o serviço, incluindo tendências locais, histórias, anúncios e sugestões de pessoas para interagir.

No que concerne aos dados de registro, um ponto merece destaque: a plataforma expõe que recebe informações quando há qualquer tipo de interação com os serviços, mesmo que não tenha sido criada uma conta. Esses dados incluem informações como o endereço de IP, o tipo de navegador, o sistema operacional, a página da web de origem, páginas da web visitadas, localização, operadora de telefonia celular, informações de dispositivo, termos de pesquisa e informações de cookies.

A rede social afirma que tais dados são usados para fazer inferências sobre os tópicos pelos quais o usuário pode estar interessado, a idade dele, bem como o idioma falado, ajudando a personalizar o conteúdo mostrado a ele, inclusive com anúncios.

Entretanto, tal coleta não encontra respaldo na legislação sobre dados pessoais, uma vez que, além de contrariar os princípios da finalidade, adequação e necessidade, uma vez que não há consonância entre o propósito e a quantidade de dados tratados, viola a necessidade de consentimento para o tratamento, visto que o visitante sequer concordou com os termos de uso e as políticas do Twitter.

Assim, tal previsão contraria o disposto no inciso I, art. 7º, bem como nos incisos I, II e III do art. 6º, ambos da Lei 13.709/2018.

Os dados pessoais poderão ser vendidos não apenas nos casos de fusão, aquisição ou reorganização, como também quando a plataforma estiver envolvida em um processo de falência ou de venda de ativos.

Quanto aos mecanismos de controle do usuário sobre os seus dados pessoais, o Twitter garante o acesso e a correção desses dados a qualquer momento. Também são fornecidas ferramentas para fazer objeção, restringir ou retirar o consentimento, quando aplicável, para o uso dos dados fornecidos, bem como mecanismos de portabilidade. Ademais, nos casos de exclusão, os dados de registro são armazenados por no máximo 18 meses.

Todas essas ferramentas podem ser acessadas por meio de links presentes na política de dados, o que facilita o acesso e, consequentemente, o controle exercido pelo usuário.

Dessa forma, diferente das outras redes sociais já analisadas, o Twitter não exige do usuário o consentimento integral sobre os termos expostos nas suas políticas, o que viabiliza o acesso ao recurso mesmo que não haja concordância total com o seu conteúdo.

Na parte final do texto da política de dados, estão presentes os dados dos controladores conforme o país de residência do usuário, além de informações sobre a autoridade supervisora local nos casos em que tiver alguma preocupação acerca do uso dos seus dados.

CONCLUSÃO

O presente trabalho teve como objetivo principal a análise da base legal do consentimento, dado pelo usuário por meio do aceite nos termos e condições de uso de alguns provedores de aplicações de Internet, necessário para que ele possa utilizá-los.

Para isso, foi necessário contextualizar o debate acerca das mudanças ocasionadas pelo advento da Internet e, principalmente, das redes sociais, que proporcionaram uma revolução abrupta, elevando o papel de individuo telespectador, na época em que a televisão e rádio eram os meios de comunicações oficiais, para protagonista de mudanças sociais, devido aos mecanismos de participação propiciados por elas.

Tendo em vista esse paradigma, o Direito, sempre na contramão das inovações ocorridas, precisou se adaptar a nova realidade que surgia. Entretanto, as regulações precisas e fechadas, destinadas a cercar todo e qualquer tipo de circunstância, vêm se mostrando insuficientes para resguardar a dinamicidade dos novos direitos, tal como o da proteção de dados pessoas.

Antes, a defesa da privacidade resumia-se ao "direito de ser deixado só", numa visão individualista, na qual a abstenção do Estado ou de terceiros era o suficiente para que tal direito permanecesse resguardado. No entanto, a realidade que vivemos não permite que o Direito deixe de exercer um papel positivo nesse sentido, atuando para resguardar os direitos da camada mais vulnerável nesse processo: os usuários.

Assim, com um atraso considerável em relação às legislações de outros países, o Brasil promulgou a Lei Geral sobre Proteção de Dados no final de 2018, que passará a produzir efeitos apenas em 2020, caso sua vacatio legis não seja prorrogada[71]. Contudo, o mercado brasileiro vem mostrando um progresso muito lento frente à necessidade em se adaptar às inúmeras regras previstas na nova legislação, o que abrirá margem para que a Autoridade Nacional de Proteção de Dados brasileira possa atuar.

A nova legislação sobre dados pessoais permite ao usuário um papel mais efetivo no

[71] Nesse sentido, o Projeto de Lei da Câmara nº 5762/2019 propõe prorrogar a data da entrada em vigor de dispositivos da LGPD para 15 de agosto de 2022.

controle das informações fornecidas por ele, com a previsão de direitos para exercício do titular de dados, dando concretude à autodeterminação informativa. E, nesse sentido, o consentimento, defendido por muitos doutrinadores como o vetor central do princípio, ganhou adjetivações novas para conferir validade ao seu fornecimento, tais como "livre", "informado", "inequívoco" e "específico".

Com relação a esse aspecto, é necessário salientarmos que nenhuma das plataformas analisadas no estudo de caso está em perfeito acordo com o previsto pela legislação. Começando pelo adjetivo "livre", em todas elas é exigido o consentimento para que a utilização do serviço ocorra sem oferecer ao usuário mecanismos didáticos que informem o poder de escolha entre o que será tratado ou não. Ao assinalar o *opt in*, o indivíduo concorda com o seu formato de "tudo ou nada".

Além disso, com exceção do Facebook, todos os termos e condições de uso das plataformas possuem vocabulário denso, com estipulações contratuais de difícil compreensão para o público leigo e termos genéricos que não demonstram com clareza a finalidade para qual o dado será utilizado, como “melhorar sua experiência” e “criar produtos personalizados”. Isso impede que o consentimento seja adjetivado como “informado” e “inequívoco”, uma vez que é fornecida uma concordância que mais funciona como um cheque em branco.

Quanto aos dados sensíveis, todas as plataformas demonstram grau adequado de proteção. Entretanto, no que tange à transferência internacional de dados para países com grau menor de proteção, mesmo sendo necessário um duplo consentimento, específico para o tratamento de dados dessa natureza, os provedores entendem que a concordância dada inicialmente é o necessário para permitir.

Ademais, ressalta-se que, com exceção do LinkedIn, é do conhecimento de toda comunidade a utilização das redes sociais por crianças e adolescentes, o que implicaria na obtenção de um consentimento em destaque e específico dado por pelo menos um dos pais para que o tratamento desses dados pudesse ocorrer. Ocorre que, mesmo com perfis infantis que ultrapassam os milhões de seguidores, as plataformas não oferecem mecanismos compatíveis com a tecnologia disponibilizada de verificação acerca da veracidade das informações dadas, o que coloca em risco o seu melhor interesse e contraria o disposto na

legislação.

De toda forma, considerando que a legislação ainda não entrou em vigor, será necessário que o consentimento dado pelos titulares seja renovado, uma vez que as diretrizes atuais estão em desacordo com estipulado pela LGPD. Nessa hipótese, caberá ao controlador ou operador contatar os titulares através de um e-mail, por exemplo, alertando sobre as mudanças decorrentes da LGPD e solicitando que os novos termos de uso e política de privacidade sejam lidos e consentidos, nos casos de concordância.

Dentro desse contexto, a legislação preocupou-se mais com a adjetivação do consentimento do que com os mecanismos de operacionalização dele, o que propiciou às empresas a criação de um campo de regulamentação que só engloba os seus interesses, como os próprios termos de uso e políticas de privacidade.

Assim, as formas de obtenção mais utilizadas pelas plataformas, como no caso de todas as analisadas por esse trabalho, que se utilizam da caixa *opt in*, mitigam a ideia de controle e acesso pelo usuário quanto às informações colhidas e tratadas, bem como suas finalidades. No que diz respeito ao *"privacy by default"*, as caixas das quatro plataformas estavam sem assinalação prévia, requerendo ação positiva do usuário para validar sua concordância.

Além disso, as redes sociais não propiciam mecanismos eficazes para a tutela de todos os direitos previstos no art. 18, LGPD, como, por exemplo, o direito de revogação do consentimento. Com exceção do Twitter e LinkedIn, nenhuma outra plataforma direciona ao usuário o que deve ser feito nos casos em que se deseja excluir, retificar, opor, restringir, dentre outros direitos. Nesse sentido, um ponto positivo, vigente no Twitter, é a presença de *links* no decorrer dos seus termos, que facilitam o acesso aos mecanismos de controle do usuário.

Nos tópicos de eliminação de dados, também não são especificadas informações abrangentes acerca do tempo levado para sua exclusão, pautando-se apenas em informar os casos em que eles serão resguardados por interesse público ou dever legal e regulatório. Por exemplo, o Facebook só dispõe de informações acerca do tempo nos casos de registro de pesquisa e de cópia de documentação para verificação da conta; já o Twitter prevê apenas quanto aos dados de registro.

Por vezes, o tempo dado era desencontrado entre os termos de uso e a política de privacidade da plataforma. Assim, na dúvida, deve-se aplicar o menor prazo.

Com relação à publicidade direcionada, todas as plataformas estudadas realizam e as suas previsões quanto à finalidade, permissividade e compartilhamento são extremamamente genéricas, o que deve implicar ao usuário uma constante desconfiança.

Nos casos de alterações nas disposições dos termos de uso e não concordância do usuário, o Facebook, o LinkedIn, o Twitter e o Instagram indicam como única alternativa a exclusão da conta. Isso demonstra a arbitrariedade das plataformas e a desproporcionalidade entre os dois lados da balança dessa relação contratual, visto que fere totalmente a capacidade do usuário em questionar qualquer cláusula contida no documento.

As disposições presentes nos termos do Twitter e do LinkedIn vinculam tanto usuários quanto visitantes, principalmente para fins de marketing. Esse modelo evidencia que a concordância não é requisito primordial para que ocorra coleta, uso e compartilhamento de dados, uma vez que o mero acesso já possibilita isso.

Por outro lado, apenas essas duas redes sociais prevêem, no texto da política de dados, os dados dos controladores conforme o país de residência do usuário, além de informações sobre a autoridade supervisora competente nos casos em que o usuário tiver alguma preocupação acerca do uso dos seus dados.

Diante de todo o exposto, podemos concluir que o caminho de adaptação entre as redes sociais estudadas e a Lei Geral de Proteção de Dados será longo. Tendo em vista as disposições estudadas e a sua conformidade com a legislação, poucas foram aquelas que forneciam mecanismos adequados e que respeitassem o direito do usuário.

Aliás, os próprios termos de uso e as políticas de privacidade não são mais recursos satisfatórios numa perspectiva de autodeterminação informacional, uma vez que eles mitigam a proteção ao usuário sob o prisma do consentimento, através de disposições estabelecidas por meio de um contrato de adesão. Ademais, levando em conta a massificação da utilização de um número relevante de redes sociais, a leitura de todas as previsões individualizadas torna-se

inviável.

Por exemplo, o LinkedIn expõe que, tendo em vista a dinâmica que os serviços oferecidos necessitam para apresentar novos recursos, talvez seja exigida a coleta de novas informações. Caso sejam coletados dados pessoais substancialmente diferentes ou alterada de forma significativa o uso desses dados, o usuário será notificado. Ou seja, primeiro haverá a coleta e, posteriormente, a obtenção de um novo consentimento, o que não faz sentido sob a ótica da proteção de dados.

Dessa forma, entendemos necessário o estabelecimento de uma ideia de privacidade contextual que varie o tratamento dos dados de acordo com o fluxo informacional pelo qual eles estão sendo oferecidos, com a possibilidade de fornecimento para outro contexto com a obtenção de consentimentos destinados a isso e, desde que, não fujam da finalidade pela qual foi inicialmente fornecida. Outrossim, a legislação precisa estabelecer núcleos duros de atuação, nos quais, mesmo que haja a concordância do usuário, o seu fornecimento e tratamento não deverá ocorrer.

REFERÊNCIAS

ALEMANHA. *Hessisches Datenschutzgesetz*, de 07 janeiro de 1999.

ARGENTINA. Ley Nº 25.326, de 04 de outubro de 2000.

AÚSTRIA. *Datenschutzgesetz*, de 18 de outubro de 1978.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e o limite do consentimento.** Rio de Janeiro: Forense, 2019.

_____. **Xeque-Mate**: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. GPoPAI/USP, São Paulo, jul/2015 Disponível em: https://gpopai.usp.br/wordpress/wpcontent/uploads/2016/07/XEQUE_MATE_INTERATIVO2.pdf. Acesso em: 29/08/2018.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. **Diário Oficial da União**, Brasília, DF, 15 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

_____. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União**, Brasilía, DF, 24 de abril de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

_____. Projeto de Lei da Câmara nº 5762/2019. Altera a Lei nº 13.709, de 2018, prorrogando a data da entrada em vigor de dispositivos da Lei Geral de Proteção de Dados Pessoais – LGPD – para 15 de agosto de 2022. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1828120&filename=PL+5762/2019.

_____. Superior Tribunal de Justiça. Recurso Especial nº 595.600/SC. Direito civil. Direito de imagem. *Topless* praticado em cenário público. Recorrente: Maria Aparecida de Almeida Padilha. Recorrido: Zero Hora Editora Jornalística S/A. Relator: César Asfor Rocha. Brasília, 18 de março de 2004.

_____. Superior Tribunal Federal. Agravo em Recurso Extraordinário nº 65777/SP. Garantias Constitucionais. Proteção da Intimidade e Sigilo de Dado. Recorrente: Município de São Paulo. Recorrido: Ana Maria Anbreu Lacambra. Relator: Ministro Teori Zavaskci. Brasília, 23 de abril de 2015.

_____. Superior Tribunal Federal. Recurso Extraordinário nº 673707/MG. Habeas Data. Recorrente: José Roberto Roca Guimarães e outros. Recorrido: União. Relator: Ministro Luiz Fux. Brasília, 17 de junho de 2015.

CHILE, Ley Nº 19.628, de 28 de agosto de 1999.

COLÔMBIA, Ley Estatutaria Nº 1.581, de 17 de outubro de 2012.

CONSELHO DA EUROPA. Convenção nº 108 para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal. Estrasburgo, 28 de janeiro de 1981. Disponível em: http://www.gddc.pt/direitos-humanos/textosinternacionais-dh/tidhregionais/conv-tratados-28-1-981-ets-108.html. Acesso em: 29/08/2018.

_____. REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Européia, Bruxelas, Bélgica. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Acesso em: 29/08/2018.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. Espaço Jurídico, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: http://editora.unoesc.edu.br/index.php/espacojuridico/article/view/1315. Acesso em: 29/08/2018.

_____. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

_____. **Reflexões sobre proteção de dados pessoais em redes sociais. Revista Internacional de Protección de Datos Personales. n. 1. Dezembro 2012. Disponível e**m: http://editora.unoesc.edu.br/index.php/espacojuridico/article/view/1315. Acesso em: 01/08/2018.

EM 2062, invenções do desenho Os Jetsons serão ultrapassadas. **TERRA**, 29 de outubro de 2012. Disponível em: https://www.terra.com.br/noticias/tecnologia/em-2062-invencoes-do-desenho-os-jetsons-serao-ultrapassadas,2d08a6882596b310VgnCLD200000bbcceb0aRCRD.html. Acesso em: 09 de agosto de 2019.

ESPANHA. Constitución española, de 29 de agosto de 1978.

GRAGNANI, Juliana. Um Brasil dividido e movido a notícias falsas: uma semana dentro de 272 grupos políticos no WhatsApp. **BBC News Brasil**, Londres, 05 de outubro de 2018. Disponível em: https://www.bbc.com/portuguese/brasil-45666742. Acesso em: 09 de agosto de 2019.

HARARI, Yuval Noah. **Homo Deus:** uma breve história do amanhã. Tradução: Paulo Geiger. 1ª edição. São Paulo: Companhia das Letras, 2006.

HOLSTON, James. **Rebeliões metropolitanas e planejamento insurgente no século XXI | Insurgent cities and urban citizenship in the 21st Century**. Revista Brasileira de Estudos Urbanos e Regionais, [S.l.], v. 18, n. 2, p. 191, ago. 2016. ISSN 2317-1529. Disponível em: http://rbeur.anpur.org.br/rbeur/article/view/5162. Acesso em: 09/08/2019. doi:http://dx.doi.org/10.22296/2317-1529.2016v18n2p191.

LIMA, C. C. C.; MONTEIRO, R. L. **Panorama brasileiro sobre a proteção de dados pessoais: discussão e análise comparada.** AtoZ: novas práticas em informação e conhecimento, Curitiba, v. 2, n. 1, p. 60-76, jan./jun. 2013. Disponível em: http://www.atoz.ufpr.br. Acesso em: 01/08/2018.

LUXEMBURGO, 24 de Outubro de 1995. Directiva 95/46/CE do Parlamento Europeu e do Conselho, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046.
Acesso em: 12/08/2019.

MAGRANI, Eduardo. **A internet das coisas.** Rio de Janeiro: FGV Editora, 2018. p. 91-107.

Mapa da Proteção de Dados Pessoais ao redor do mundo, elaborado pela Comissão Nacional de Informática e Liberdade - CNIL/França. Disponível em: https://www.serpro.gov.br/lgpd/menu/arquivos/mapa-sobre-protecao-de-dados-no-mundo. Acesso em: 12/09/2019

Markoff, John. **Entrepreneurs see a web guided by common sense.** The New York Times, 2006. Disponível em: https://www.nytimes.com/2006/11/12/business/12web.html. Acesso em: 09/08/2019.

MONTEIRO, Renato Leite**. Lei Geral de Proteção de Dados e GDPR**: histórico, análise e impactos. Disponível em: https://baptistaluz.com.br/wp-content/uploads/2019/01/RD-DataProtection-ProvF.pdf. Acesso em: 06/08/2019.

OCDE. Diretrizes da OCDE sobre a proteção da privacidade e fluxos transfronteiriços de dados pessoais. **OECD Publishing**, Paris. Disponível em: https://doi.org/10.1787/9789264196391-en.

PARAGUAI. Ley Nº 1682, de 16 de janeiro de 2001

PERU. Ley Nº 29.733, de 03 de julho de 2011.

PORTUGAL. Comissão Nacional de Protecção de Dados. Parecer n.º 25/2019, de 10 de maio de 2019.

PORTUGAL. Constituição da República Portuguesa, de 25 de abril de 1976.

RODOTÀ, Stefano. **A vida na sociedade de vigilância - a privacidade hoje.** Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro. Renovar, 2008.

SISTEMA de reconhecimento facial da PM do RJ falha, e mulher é detida por engano. **Portal de Notícias G1**, 2019. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml. Acesso em: 14/11/2019.

SUÉCIA. *Sw. Datalagen*, de 11 de maio de 1973.

TATEOKI, Victor Augusto. A proteção de dados pessoais e a publicidade comportamental. **Revista Juris UniToledo**, Araçatuba, SP, v. 02, n. 01, p. 62-75, jan./mar. 2017. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/113-2706-1-pb.pdf. Acesso em: 01/08/2018.

TEFFÉ, Chiara Spadaccini de. Consentimento e Proteção de Dados Pessoais na LGPD. In: TEPEDINO, G. (Coord.); Frazão, A. (Coord.); OLIVA, M. Milena (Coord.). **Lei Geral de proteção de dados pessoais e suas repercussões no Direito Brasileiro.** Revista dos Tribunais, 2019.

URUGUAI, Ley Nº 18.331, de 18 de agosto de 2008

VENAGLIA, Guilherme. Após crítica de bolsonaristas, Moro volta atrás em nomeação de Ilona Szabó. **VEJA**, 28 de fevereiro de 2019. Disponível em:

https://veja.abril.com.br/politica/apos-critica-de-bolsonaristas-moro-volta-atras-em-nomeacao-de-ilona-szabo/. Acesso em: 09/08/2019.

ZSPR.421.7.2019. Personal Data Protection Office. Varsóvia, 16 de outubro de 2019. Disponível em: https://uodo.gov.pl/decyzje/ZSPR.421.7.2019. Acesso em: 14/11/2019.